VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA PODNIKATELSKÁ
FACULTY OF BUSINESS AND MANAGEMENT

ÚSTAV INFORMATIKY
INSTITUTE OF INFORMATICS

ZAVEDENÍ ISMS PRO ZÁKLADNÍ ŠKOLU
IMPLEMENTATION OF ISMS AT ELEMENTARY SCHOOL

DIPLOMOVÁ PRÁCE
MASTER'S THESIS

AUTOR PRÁCE — **Bc. Marek Hensl**
AUTHOR

VEDOUCÍ PRÁCE — **Ing. Petr Sedlák**
SUPERVISOR

BRNO 2017

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
FAKULTA PODNIKATELSKÁ

Zadání diplomové práce

Ústav:	Ústav informatiky
Student:	**Bc. Marek Hensl**
Studijní program:	Systémové inženýrství a informatika
Studijní obor:	Informační management
Vedoucí práce:	**Ing. Petr Sedlák**
Akademický rok:	2016/17

Ředitel ústavu Vám v souladu se zákonem č. 111/1998 Sb., o vysokých školách ve znění pozdějších předpisů a se Studijním a zkušebním řádem VUT v Brně zadává diplomovou práci s názvem:

Zavedení ISMS pro základní školu

Charakteristika problematiky úkolu:

Úvod
Vymezení problému a cíle práce
Teoretická východiska
Analýza současného stavu
Vlastní návrh řešení
Zhodnocení a přínosy práce
Závěr
Seznam použité literatury
Přílohy

Cíle, kterých má být dosaženo:

Pro vybranou základní školu na základě analýzy vypracujte metodický postup pro zavedení ISMS.

Základní literární prameny:

ČSN ISO/IEC 27001, Informační technologie – Bezpečnostní techniky – Systémy managementu bezpečnosti informací – Požadavky. Praha: Český normalizační institut, 2014.

ČSN ISO/IEC 27002, Informační technologie – Bezpečnostní techniky – Systémy managementu bezpečnosti informací – Soubor postupů. Praha: Český normalizační institut, 2014.

DOUCEK, Petr. Řízení bezpečnosti informací: 2. rozšířené vydání o BCM. 2., přeprac. vyd. Praha: Professional Publishing, 2011. ISBN 978-80-7431-050-8.

ONDRÁK, Viktor, Petr SEDLÁK a Vladimír MAZÁLEK. Problematika ISMS v manažerské informatice. Brno: Akademické nakladatelství CERM, 2013. ISBN 978-80-7204-872-4.

Termín odevzdání diplomové práce je stanoven časovým plánem akademického roku 2016/17.

V Brně, dne 28. 2. 2017

L.S.

doc. RNDr. Bedřich Půža, CSc.
ředitel

doc. Ing. et Ing. Stanislav Škapa, Ph.D.
děkan

ABSTRAKT

Diplomová práce se zabývá problematikou, analýzou a návrhem systému řízení bezpečnosti informací na základní škole. Práce vychází z dlouhodobé zkušenosti se školou a z komunikace s představiteli školy. V práci jsou popsány jak teoretické základy, tak konkrétní stav, nedostatky a na ně navazující vlastní návrh.

ABSTRACT

This diploma's thesis deals with information security management system on elementary school. This work is based on long time experience with chosen school and on communication with representatives of elementary school. In this thesis are teoretical basics, specific state, shortcomings and proposed or recommended solutions.

KLÍČOVÁ SLOVA

ISMS, bezpečnost informací, ISO/IEC 27001

KEY WORDS

ISMS, Information Security, ISO/IEC 27001

BIBLIOGRAFICKÁ CITACE

HENSL, M. *Zavedení ISMS pro základní školu.* Brno: Vysoké učení technické v Brně, Fakulta podnikatelská, 2017. 83 s. Vedoucí diplomové práce Ing. Petr Sedlák.

ČESTNÉ PROHLÁŠENÍ

Prohlašuji, že předložená diplomová práce je původní a zpracoval jsem ji samostatně.

Prohlašuji, že citace použitých pramenů je úplná a že jsem ve své práci neporušil autorská práva (ve smyslu zákona č. 121/2000 Sb., o právu autorském a o právech souvisejících s právem autorským).

V Brně dne 20. května 2017 ……...

Podpis

PODĚKOVÁNÍ

Chtěl bych touto cestou poděkovat panu Ing. Petrovi Sedlákovi za možnost vypracování diplomové práce pod jeho dohledem a za jeho cenné připomínky k diplomové práci a připomínky během studia.

OBSAH

ÚVOD

V době, kdy přístup k elektronickým zařízením je stále snadnější a technologie stále modernější, je potřeba o to více myslet na bezpečnost informací a dat, neboť i útoky na citlivá data jsou stále častější a pro útočníky dostupnější. Pro organizace pak je možné si nechat zavést tzv. ISMS neboli systém řízení bezpečnosti dat, resp. zavést takové opatření, které sníží rizika ohrožení informací na minimum. Taková opatření jsou pak tvořena dle normy ISO/IEC. Informace jsou dnes pro všechny organizace, tedy i školy, velmi důležitým aktivem, to je třeba si uvědomovat.

Problémem bývá právě značná nevzdělanost uživatelů v oblasti ochrany nejen proti kybernetickým útokům a zároveň si lidé často neuvědomují následky svého chování na internetu a ve svém okolí. Informace musí být chráněné také z pohledu elektronických zařízení, jako jsou servery, počítačové sítě a koncové stanice, ze kterých může útočník získat důležité informace.

VYMEZENÍ PROBLÉMŮ A CÍLE PRÁCE

Cílem diplomové práce je vypracování analýzy současného stavu školy a nalezení jejich slabých míst z pohledu informační bezpečnosti. Na tuto analýzu je dále navrhnuté řešení systému řízení bezpečnosti dat, které odpovídá normě ISO/IEC 27001. Poskytnuté řešení může sloužit vedení školy jako návod pro zavedení ISMS, které je dnes stále častější tématikou a zároveň jako rozšíření vědomostí právě v pohledu na informační bezpečnost a zdůraznit její důležitost.

1 TEORETICKÁ VÝCHODISKA PRÁCE

Pro správné pochopení vlastního návrhu práce je potřeba znát alespoň základní pojmy, které se týkají bezpečnosti informací. V této kapitole tedy budou vysvětleny pojmy, ze kterých se vychází v analýze současného stavu a vlastním návrhu.

1.1 Základní názvosloví a pojmy

ICT (Information and Communication Technology) – Informační a komunikační technologie

IS (Information System) – Informační systém

Informace – Informace popisuje reálné prostředí, zjišťuje jeho stav a procesy v něm probíhající ve formě údajů.

Informace je v informatice tvořena kódovanými daty

Data – Data jsou předmětem operací v informatice, resp. jsou zdrojem pro komunikaci, přípravu, zpracování a vyhodnocování informací.

Dostupnost – V požadovaný okamžik je zajištěn přístup k informacím oprávněnému uživateli.

Integrita – Zajištění úplnosti a správnosti dodávaných informací.

Důvěrnost – Přístup k informacím je zajištěn pouze oprávněnému uživateli.

Tyto tři pojmy spolu tvoří tzv. CIA triádu (Confidentiality, Integrity, Availability). (1)

Obrázek 1: CIA triáda (4)

Událost a incident

“Kybernetickou bezpečnostní událostí je událost, která může způsobit narušení bezpečnosti informací v informačních systémech nebo narušení bezpečnosti služeb a sítí elektronických komunikací.” (25)
“Kybernetickým bezpečnostním incidentem je kybernetická bezpečnostní událost, která představuje narušení bezpečnosti informací v informačních systémech nebo narušení bezpečnosti služeb a sítí elektronických komunikací.“ (25)

Zranitelnost – Slabé místo konkrétního aktiva.

Hrozba – Událost, která ohrožuje bezpečnost, resp. může zneužít zranitelnosti aktiva. Rizika hrozeb lze snížit přijmutím bezpečnostních opatření. (1)

1.2 Informační bezpečnost

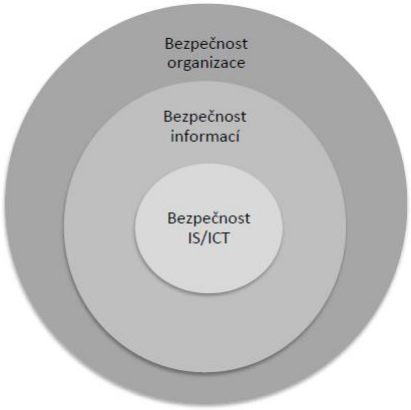
Informační bezpečnost je soubor pravidel, nástrojů a politik, které slouží k ochraně informací v digitální i fyzické formě a zajišťují tak integritu, důvěrnost a dostupnost systémů a dat.

Ve větších organizacích je k řízení informační bezpečnosti dedikovaný pracovník, vedoucí informační bezpečnosti (Chief Information Security Officer).

Informace bývají napadány nejčastěji v podobě fyzických útoků, malwaru, phishingu a ransomware.

Pro včasnou detekci, případně pro minimalizaci škody v případě napadení, je třeba mít vytvořen tzv. Incident Response Plan (IRP). IRP poskytuje instrukce k správnému chování v případě narušení dat, odstavení služby, narušení firewallu nebo napadení virusem. (1), (2)

Z níže uvedeného obrázku lze vidět, že bezpečnost informací je úzce spojena s bezpečností organizace a bezpečností IS/ICT



Obrázek 2: Bezpečnost (5)

1.3 ISMS

Název vychází z anglického Information Security Management system neboli Systém řízení informační bezpečnosti.

Jedná se o systematický přístup ke správě citlivých informací subjektu tak, aby informace zůstaly zabezpečené, to zahrnuje osoby, procesy a systémy.

Motivací zavedení ISMS je ta, že společnost nebo organizace si je jistá správným nasazením řešení bezpečností informací, procesů a zároveň snížením rizika při nečekaných událostech.

ISMS je založeno na modelu Demingův cyklus s následujícími etapy:

- Ustanovení ISMS
- Zavádění a provoz ISMS
- Monitorování ISMS
- Údržba a zlepšování (1)

1.3.1 Postupy zavádění ISMS

Aby bylo prosazení a zavedení ISMS bez komplikací, je třeba postupovat podle předem daných pravidel, ty se dají rozdělit do čtyř bodů.

Z praktického hlediska je třeba ISMS implementovat směrem od vrchu dolů, takže prvním krokem musí být souhlas o zavádění a vytvoření požadovaného dokumentu, kde se vedení organizace zavazuje, že podporuje zavádění ISMS. Souhlas o zavádění požaduje také norma.

Druhý bod slouží k identifikaci aktiv, jejich ocenění a vytvoření analýzy rizik. K identifikaci a ocenění aktiv je zapotřebí nejdříve provést celkovou kontrolu aktiv, následně provést jejich ohodnocení z pohledu integrity, dostupnosti a důvěrnosti, a to na základě algoritmu, který hodnotu aktiv určí. Důležitou součástí zavedení ISMS je analýza rizik.

Třetím bodem je vytvoření návrhu opatření vůči rizikům, která se identifikovala v předchozím bodě. Na základě nalezených kritických míst je třeba vybrat taková bezpečnostní opatření, která umožní eliminovat nalezená rizika.

Posledním, čtvrtým bodem v zavádění ISMS je certifikace. Tato část není povinná, je pouze doporučená, neboť ISMS může fungovat aplikované i bez certifikace. Certifikace se dělí na povinnou dokumentaci a na praktické zavedení ISMS. (1)

1.4 Normy

K tomu, aby byla implementace ISMS kompletní dle PDCA cyklu, je třeba certifikovat ISMS dle platných norem. Pokud organizace respektuje bezpečnostní normy, pak je nezávislá na zařízení a dodavateli.

Názvy norem jsou zkratkami tří organizací, které se na normách podílejí.

ČSN

Jedná se o chráněné označení Českých technických norem. ČSN označuje normy svou zkratkou přidáním šestimístného čísla, kde první dvě čísla představují třídu norem, další dvě čísla označují skupinu a podskupinu normy a poslední dvojčíslí je pořadové číslo normy. V případě převzatých neboli normalizovaných norem, je značení převzato z původní normy, pouze je před označení přidána zkratka ČSN. (6)

ISO

ISO je zkratka z anglického International Organization for Standartization neboli Mezinárodní organizace pro normalizaci. Organizace se zabývá tvorbou mezinárodních

norem a dalších dokumentů, které se týkají normalizace a jsou to normy všech oborů kromě elektrotechniky. Členy ISO jsou národní normalizační organizace v daných zemích. Českou republiku zastupuje Úřad pro technickou normalizaci, metrologii a státní zkušebnictví. (7)

Obrázek 3: ISO logo (8)

IEC

IEC je zkratka z anglického International Electrotechnical Commission neboli Mezinárodní elektrotechnická komise. Jedná se o světovou organizaci, která se zabývá tvořením a publikací mezinárodních norem pro elektrotechniku, elektroniku a sdělovací techniku. (9)

Obrázek 4: IEC logo (9)

ÚNMZ

Úřad pro technickou normalizaci, metrologii a státní zkušebnictví je organizační složka státu, která zabezpečuje úkoly, které vyplývají z usnesení vlády z roku 1994 a zajišťuje proces integrace právního řádu a technických předpisů z norem mezi Českou republikou a Evropskou unií. (10)

1.4.1 ČSN ISO/IEC 27000

Norma poskytuje přehled systémů řízení bezpečnosti informací, které tvoří celý předmět norem ISMS. Norma slouží k zavedení a provozování ISMS pro všechny velikosti subjektů. ČSN ISO/IEC 27000 slouží jako podklad pro další, níže zmíněné normy.

První vydání normy bylo publikováno v roce 2009. Momentálně je k dispozici třetí vydání z roku 2016 (6)

1.4.2 ČSN ISO/IEC 27001

Norma slouží k procesu ustanovení, provozu, údržby a zlepšování systému managementu bezpečnosti informací dle PDCA cyklu, který může být aplikován na jednotlivé procesy ISMS tak, jak jsou definovány touto normou.

První vydání bylo publikováno v roce 2005 jako náhrada verze BS7799-2:2002. Poslední vydání bylo publikováno v roce 2014. (11)

1.4.3 ČSN ISO/IEC 27002

Norma obsahuje přímé a odvozené bezpečnostní opatření, které podporují dosahování převážně podnikatelských cílů a odpovědnost za jednotlivý opatření je možné přiřadit odpovídajícím osobám. Normu je také možné využít jako podklad pro vyvíjení směrnic pro řízení bezpečnosti informací, které přihlíží ke konkrétnímu prostřední a jejich rizika pro bezpečnost informací. (6)

1.4.4 ČSN ISO/IEC 27003

Norma vysvětlující proces návrhu a implementaci ISMS pomocí popisu zahájení, definování a plánování ISMS, kde výsledkem je kompletní plán pro realizaci ISMS. Dle tohoto plánu je implementace řazena do pěti etap:

- Získání souhlasu vedení se zavedením ISMS a zároveň jeho aktivní podpora
- Definice rozsahu, hranic a politik ISMS

- Provedení analýzy
- Provedení hodnocení rizik
- Návrh ISMS

1.4.5 ČSN ISO/IEC 27004

Norma, která poskytuje doporučení pro vývoj a používaní metrik a pro měření účinnosti zavedeného ISMS. Proces měření bezpečnosti informací zahrnuje procesy rozvoje metrik a měření, provádění samotného měření, analýza dat a hlášení výsledků měření. (6)

1.4.6 ČSN ISO/IEC 27005

Norma sloužící především pro management organizace, který je zodpovědný za řízení rizik v organizaci. Norma tedy obsahuje doporučení pro řízení rizik bezpečnosti informací v organizací. (6)

1.4.7 ČSN ISO/IEC 27006

Norma specifikuje požadavky a doporučení pro orgány, které provádějí audit a certifikace ISMS. Je primárně určena k podpoře procesu akreditace certifikačních orgánů, které poskytují certifikaci ISMS. (6)

1.5 Bezpečnost informací v akademickém prostředí

V akademickém prostředí řeší ISMS následující bezpečnostní politiky:

- Správa osobních dat studentů
- Správa osobních dat zaměstnanců
- Řešení objektové a přístupové bezpečnosti
- Cíle bezpečnostní politiky

Vzhledem k tomu, že škola je poskytovatelem internetu studentům, je třeba dbát na následující opatření:

- Silné zabezpečení Wi-Fi sítě (např. WPA2, AES)
- Oddělení sítě pro studenty, zaměstnance, výuku
- Autentizace a autorizace uživatelů a logování jejich aktivit
- Zavedení bezpečnostní politiky
- Dodržování IT standardů

Norma používající se v akademickém prostředí je *ČSN ISO/EIC 27000* (Systém managementu bezpečnosti informací) a *ČSN ISO/EIC 20000* (Systém managementu služeb IT). (1), (29)

1.6 PDCA cyklus

PDCA (Plan, Do, Check, Act) cyklus neboli Demingův cyklus, je čtyřbodový přístup k opakovanému kontrolování a zlepšování kvality v organizaci.

Plan (plánuj) – Část, ve které jsou popsány procesy, situace a sestavení plánu k předpokládanému zlepšení

Do (dělej) – Implementace první části, často pouze na vybraný testovací vzorek (např. malé oddělení společnosti nebo v laboratoři)

Check (kontroluj) – Kontrola a vyhodnocení zavedené změny, zdali byla úspěšná či nikoliv. V případě, že výsledek není uspokojící, je třeba se vrátit k předchozím bodům a pozměnit postup.

Act (konej) – Jedná se o plošné zavedení do praxe zavedené změny, vyhodnotit výsledky a pokračovat dalším krokem, tedy opět Plan a plánovat další potřebné zlepšení v organizaci. (3)

Obrázek 5: PDCA (12)

1.6.1 PDCA v ISMS

PDCA je upraveno i pro ISMS a obsahuje následující.

Plan

Kontext organizace

Porozumění organizaci, potřeby očekávání, stanovení rozsahu ISMS

Vůdčí role

Vůdčí role a závazky, politika v organizaci, role, odpovědnosti a pravomoci

Plánování

Opatření zaměřená na rizika, cíle bezpečnost informací

Podpora

Zdroje, komunikace, dokumentované informace

Do

Provozování

Plánování a řízení provozu, posuzování rizik, ošetření rizik bezpečnosti informací

Check

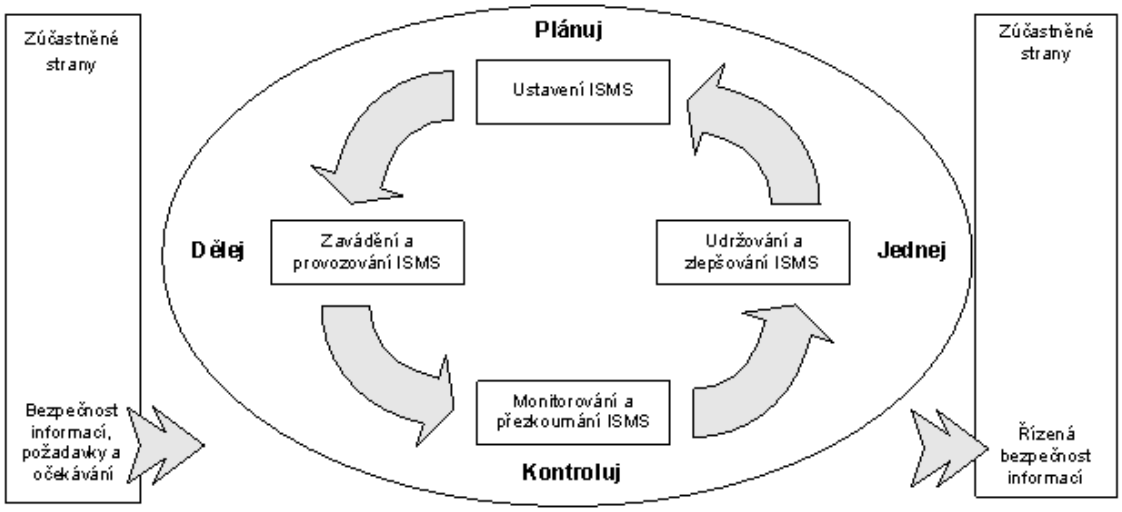
Hodnocení výkonosti

Monitorování, měření, analýza a hodnocení, interní audit, přezkoumání vedením

Act

Zlepšování

Neshody a nápravná opatření, opakované zlepšování (14)



Obrázek 6: PDCA implementováno v ISMS (15)

1.7 SAE

Česky budování bezpečnostního povědomí přeloženo z anglického Security Awareness Education.

SAE slouží ke snižování bezpečnostního rizika způsobenéjp neškolenými zaměstnanci a uživateli a zároveň ke zvyšování bezpečnostního povědomí.

Jako základ bezpečnostního povědomí může být následujících 8 bodů:

- Silné heslo
- Záloha dat
- Antivir
- Neotevírat neznámé přílohy v mailu
- Nenavštěvovat podezřelé internetové stránky
- Firewall
- Nenechávat počítač online v nepoužívané době
- Okamžité hlášení bezpečnostních incidentů (1)

Pro správné budování bezpečnostního povědomí je třeba sestavení tzv. SAE plánu, který se dá shrnout v deseti bodech:

1. Role a odpovědnosti v programu SAE

2. Stanovení cílů pro každou fázi programu

    - budování povědomí

    - školení

    - vzdělávání

    - profesní rozvoj

    - certifikace

3. Rozdělení uživatelů (analýza)

4. Vytvoření školících materiálu dle skupin uživatelů

5. Určení cíle pro každou skupinu uživatelů

6. Témata, která je třeba řešit v každé relaci či kurzu

7. Metody nasazení pro každý aspekt programu (metodiky)

8. Dokumentace, zpětná vazba a doložení o výuky

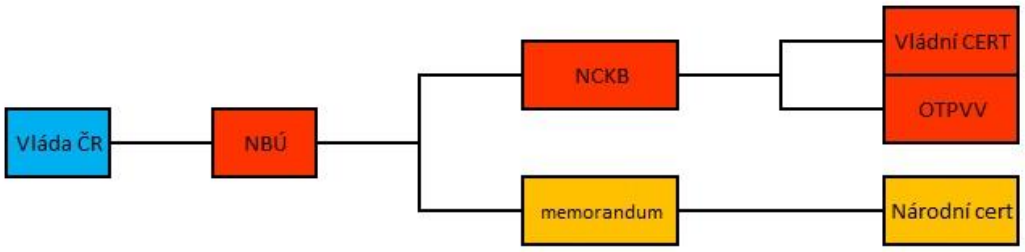
9. Vyhodnocení a aktualizace výukových materiálů

10. Četnost opakování včetně updatů materiálů

11. Kalkulace (16)

1.8 NCKB

Celým názvem se jedná o Národní centrum kybernetické bezpečnosti, je součástí Národního bezpečnostního úřadu (NBÚ). jeho základní úlohou je koordinovat spolupráci na jak národní, tak mezinárodní úrovni při předcházení kybernetických útoků. Přijímá návrhy a opatření při řešení incidentů a proti probíhajícím kybernetickým útokům. Vzniklo v roce 2014 na základě usnesení Vlády ČR ze dne 19. října 2011.



Obrázek 7: NCKB schéma (Vlastní zpracování)

Hlavní oblasti činnosti centra:

- provoz Vládního CERT (Computer Emergency Response Team) České republiky
- spolupráce s dalšími národními a mezinárodními CERT CSIRT (Computer Security Incident Response Team) týmy
- příprava bezpečnostních standardů pro jednotlivé kategorie organizací v ČR
- osvěta a podpora vzdělávání v oblasti kybernetické bezpečnosti
- výzkum a vývoj v oblasti kybernetické bezpečnosti (17)

1.9 Počítačová síť a její bezpečnost

Počítačovou síť si lze představit jako spojení dvou a více zařízení, které spolu následně mohou komunikovat, přenášet data a informace, dle stanovených norem. Nejčastějšími komunikačními uzly jsou počítače, avšak může to být jakékoliv digitální zařízení, jako je telefon, tiskárna či skener.

Bezpečnost sítě lze implementovat dle normy ISO/IEC 27033, která představuje podrobný návod na implementaci bezpečnostních mechanizmů. Cílem normy je poskytnou podrobný návod na zabezpečení správy a užívání sítí a jejich vzájemných propojení.

Skupina prvků může být považována za síť, pokud obsahuje propojovací software, síťové systémy a síťové prvky. (18)

Pro spolehlivou počítačovou síť je třeba dbát na její bezpečnost pro předcházení bezpečnostních incidentů a událostí, a proto je třeba dodržovat základní bezpečnostní opatření:

- Šifrování dat
- Kvalitní firewall
- Detekce a prevence útoku – IDS a IPS systémy
- Omezení přístupu – VPN
- Seznam povolených IP a MAC adres

Šifrování dat je proces, převádějící nezabezpečená elektronická data na šifrovaná. Tyto data je schopen dešifrovat pouze majitel dešifrovacího klíče a kdokoliv bez dešifrovacího klíče nebude schopen získané informace přečíst. (19)

1.9.1 Bezpečnost pasivní vrstvy

Jedná se o bezpečnostní opatření pasivní vrstvy počítačových sítí. Princip bezpečnosti pasivní vrstvy spočívá v instalaci monitorovacích portů na každý port kabeláže a v následném vyhodnocování signálu monitorovacího portu v zařízení. Výsledkem je hlášení všech změn propojení v reálném čase v řídící neboli management stanici. (1)

Příkladem managementu bezpečnosti pasivní vrstvy je systém NISS (Network Infrastructure Security Solutions), který definuje 3 základní stupně zabezpečení.

- Identifikátory

Stupeň, který slouží pouze k identifikaci a navigaci síťových prvků. Lze použít různé barvy při výběru konektorů, různě barevné kabely anebo barevné značkovací kroužky.

Obrázek 8: Identifikátory (20)

- Blokátory

Blokátory slouží k fyzické ochraně formou blokování portů proti připojení nebo odpojení a tím blokováním přístupu do kabelových tras. Blokátory se tedy celkem dělí na blokování portu, uzamčení portu, blokování datového boxu, blokování datových tras.

Obrázek 9: Blokátor (21)

- Klíčování konektorů

Do stupně klíčování konektorů jsou zařazeny prostředky, které znemožňují připojení skupiny kabelů do nepovolených portů. Jedná se o technické řešení s využitím klíčování konektorů. Princip spočívá ve dvou bodech

  - Neklíčovaný plug nelze zasunout do řádného klíčového konektoru
  - Klíčovaný plug nelze zasunout do neklíčovaného konektoru a ani do konektoru s jiným typem klíče. (1)

1.9.2 Firewall

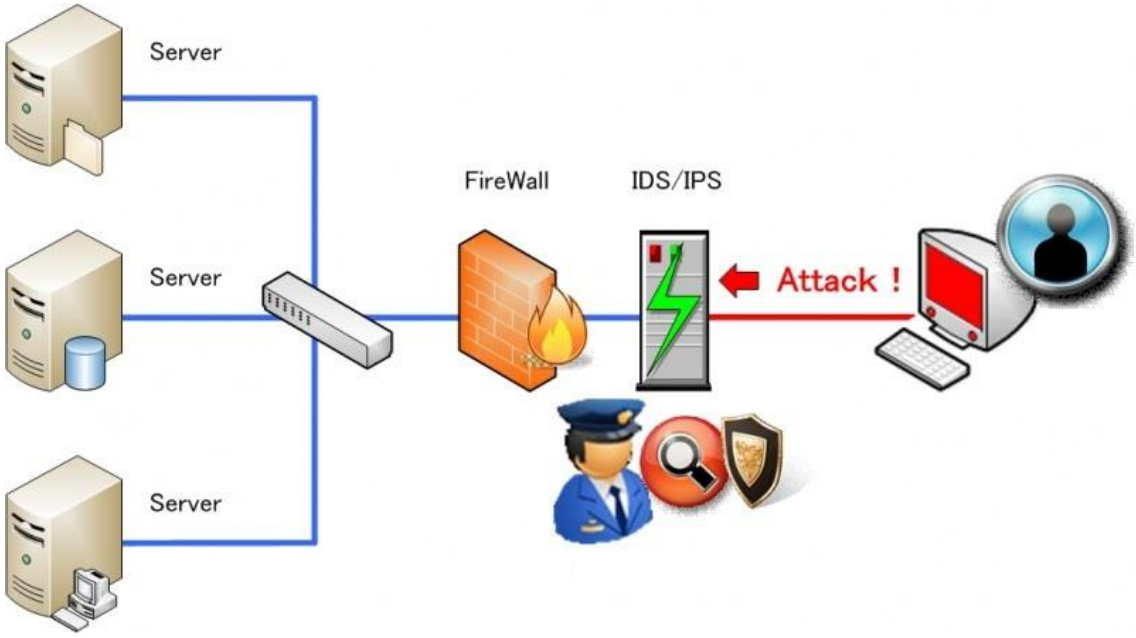
Firewall je síťové zařízení, které sleduje příchozí a odchozí tok dat a rozhoduje, zda data odpovídají předem určeným bezpečnostním pravidlům a provoz dat povolí, nebo v opačném případě provoz zakáže. Firewall existuje v softwarové a hardwarové podobě. (22)

1.9.3 IDS

IDS systémy monitorují síť a poskytují pohled na ni. Má za úkol pozorovat určité vzory, které indikují neobvyklé chování v síti. Jedná se pouze o detekční zařízení, takže nemůže poskytnou žádné zásahy proti tomuto neobvyklému chování. (22)

1.9.4 IPS

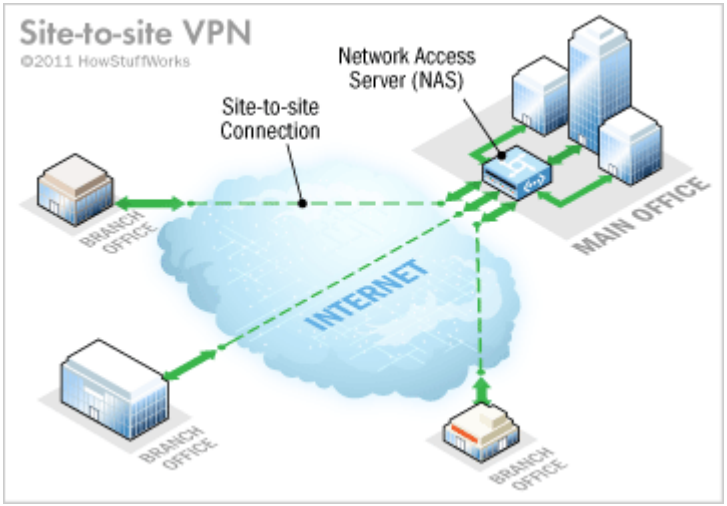
Zařízení podobné firewallu, s tím rozdílem, že IPS obsahuje seznam pravidel, které říkají, které data nepustí v provozu dále. Pokud data seznamem pravidel projdou, pak pokračují v provozu dále. Optimální IPS mají mít v sobě automaticky nastaveny stovky a tisíce filtrů pro blokování nekorektní komunikace, tomu se říká „doporučená" konfigurace. Na rozdíl od IDS systému jsou IPS systémy zařazeny přímo do síťové cesty. (22), (23)



Obrázek 10: IDS/IPS (24)

1.9.5 VPN

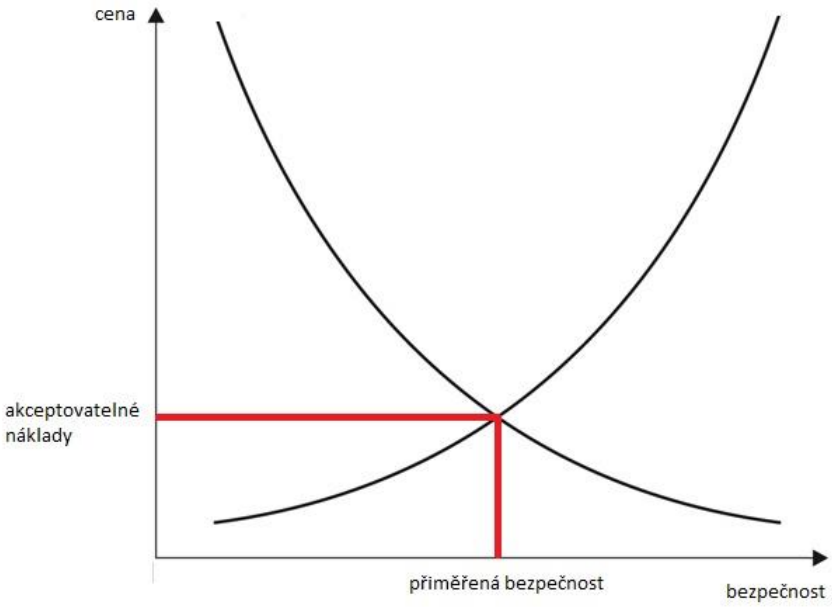
Celým názvem Virtual private network je technologie, která vytváří zabezpečené spojení v internetu (veřejné spojení) tím, že je spojuje do logické skupiny. Zařízení spolu následně mohou komunikovat tak, jako by byly připojeny v jedné privátní síti. Pro vstup do takové VPN musí zařízení obsahovat digitální certifikát nebo jiný způsob k autentizaci. (25)



Obrázek 11: VPN (26)

1.10 Přiměřená bezpečnost

Každá společnost nebo objekt má vlastní hodnotu a podle toho by mělo vypadat jeho zabezpečení. Absolutní bezpečnost je téměř nedosažitelná anebo by stála neúměrně velké množství nejen finančních prostředků, a i tak by časem rizika vznikala narušení bezpečnosti. Přiměřená bezpečnost nám říká, že bychom měli vložit finanční prostředky ke snížení dopadů rizik přiměřeně k hodnotě objektu nebo společnosti. (1)



Obrázek 12: Přiměřená bezpečnost (Vlastní zpracování)

1.11 ITIL

Celým názvem Information Technology Infrastructure Library je knihovna nejlepších zkušeností z oboru řízení služeb informačních technologií. Knihovna je spravována organizací Office of Government Commerce a je šířena prostřednictvím knih, konzultací, CD a certifikací. V současné době existuje pět ústředních publikací:

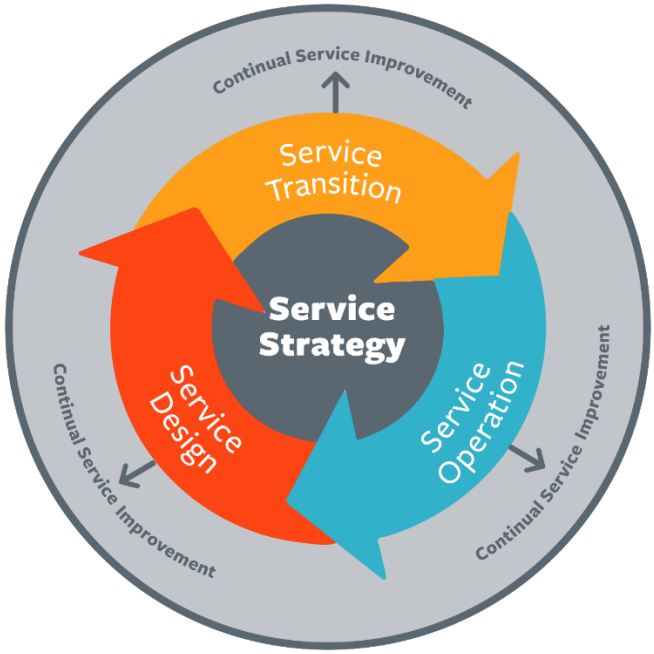
- Service Strategy
- Service Design
- Service Transition
- Service Operation
- Continual Service Improvement

Poslední aktualizace je z roku 2011 a obsahuje celkem 26 procesů, z nichž nejdůležitější jsou následující:

- Incident management
- Event management
- Request fulfilment

- Access management
- Problem management
- Service asset and configuration management
- Change management
- Release and deployment management
- IT service continuity management
- Availability management
- Service level management
- Financial management for IT services

Jedná se tedy pouze o řadu doporučení a jen výjimečně je něco striktně předepisováno. Vzhledem k tomu, že se jedná o rámec, nikoliv metodiku, nejsou jednotlivé prvky popsány detailně, ale pouze dává rámcové návody, jak reagovat na specifické situace. (29)



Obrázek 13: ITIL (27)

1.12 Cloud computing

Jedná se o poskytování služeb nebo programů, které jsou uloženy na serverech s tím, že uživatelé k nim mají vzdálený přístup pomocí dané aplikace nebo webového prohlížeče.

Výhodou cloudu je relativně jednoduchá správa, vzdálená podpora, možný vyšší výkon a finanční úspory. Nevýhodou pak může být velká závislost na poskytovateli cloudu, možné nebezpečí uložených dat, nutnost připojení k internetu nebo právní problémy při využívání cloudu, který má servery v cizích zemích.

Rozdělení cloudu:

- Veřejný

Jedná se o takový typ cloudu, kde je služba poskytována široké veřejnosti. Veřejný cloud může být zdarma, např. financován reklamami, nebo placený a dle toho poskytovatel nastavuje zpřístupněné funkce a služby. Příkladem mohou být dnes populární textové nebo zvukové programy, např. Skype.

- Soukromý

Cloud, který je poskytován pouze dané organizaci.

- Hybridní

Speciální typ cloudu, který je kombinací soukromého a veřejného. Navenek vystupují jako jeden cloud, který je propojený standardizačních technologií

- Komunitní

Cloud, který je sdílen mezi více organizací, které mají zpravidla stejnou bezpečnostní politiku nebo obor činnosti.

Obrázek 14: Cloud schéma (28)

2 ANALÝZA SOUČASNÉHO STAVU

V této části diplomové práce bude představena analýza současného stavu, tedy současný stav informační bezpečnosti na vybrané základní škole. V kapitole se vychází z informací přímo od IT správce a ředitele základní školy.

Analýza bude dále sloužit jako podklad k vlastnímu návrhu

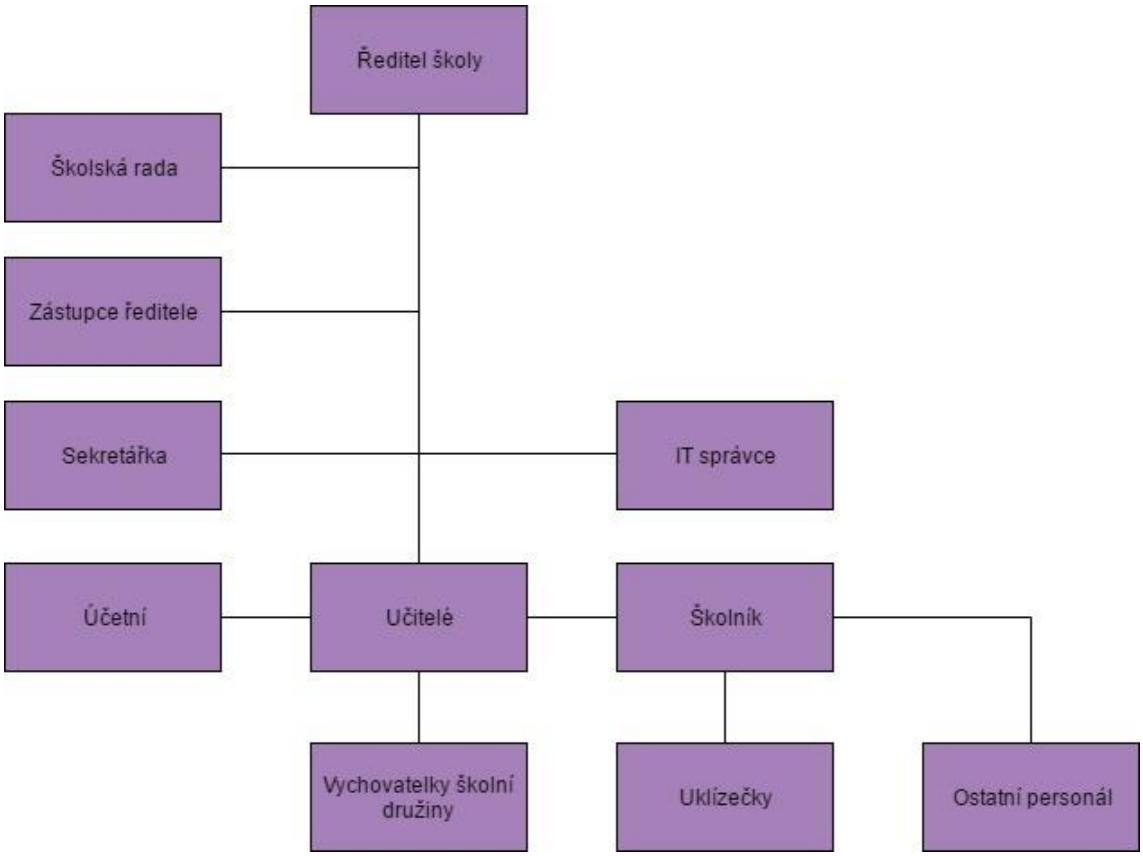
2.1 Základní charakteristika organizace

Základní škola se nachází v Jihomoravském kraji, kde primárně slouží k vyučování žáků devíti ročníků. Součástí je i školní družina a školní jídelna. Školní družina slouží k mimoškolním aktivitám před a po povinné školní docházce a také k pořádání příležitostných akcí. Momentálně jsou díky rostoucímu zájmu žáků a rodičů o školní družiny jsou nyní obsazeny tři učebny. Zřizovatelem je město.

Všechny části školy jsou situovány v jedné budově, která je rozdělená do tří křídel – pravé, střední a levé. Do školy pravidelně dochází téměř 800 studentů, kteří postupně prochází 9 stupňů, každý stupeň má třídy A, B, C, D a zaměstnává přes 60 zaměstnanců.

2.2 Organizační struktura

Vedoucím školy je ředitel, který má v organizační struktuře pod sebou školskou radu, kterou tvoří 9 zaměstnanců školy, zástupce ředitele, IT správce a sekretářku. Na dalším stupni organizační struktury jsou na stejné úrovni mzdová účetní, učitelé a dva školníci. Součástí organizační struktury jsou i vychovatelky školní družiny, které jsou v současné době 4. Uklízečky a ostatní personál, jako jsou kuchařky, spadají v organizační struktuře pod pozici školníka.



Obrázek 15: Organizační struktura

2.3 Technické vybavení objektu

V této části bude popsán současný stav z pohledu technické vybavenosti školy – hardware a software.

2.3.1 Hardware

Tato část obsahuje popis hardwaru školy, který se vztahuje k bezpečnosti informací dle výše uvedených norem a pravidel.

Stolní počítače a notebooky pro studenty

V budově základní školy se nachází tři učebny, které primárně slouží k výuce ICT. V učebnách je dohromady 95 počítačů a část z nich jsou notebooky. Počítačů je více odlišných typů a značek, z důvodu různých časových odstupů a díky výběrovému řízení. To se koná pravidelně při nákupu sady počítačů a jiných zařízení, kde by byl výběr konkrétních značek nebo modelů porušením procesu výběrového řízení.

Žáci mají k dispozici také šest počítačů na chodbě, ke kterým mají přístup během přestávek. Tyto počítače bývají nejstarší a nejméně potřebné. Z toho důvodu jsou přístupné všem studentům, kde jejich zacházení s PC neodpovídá slušnému zacházení.

Obrázek 16: Počítač v ICT učebně

Obrázek 17: Počítače na chodbě pro žáky

Notebooky pro učitele

Každý učitel má k dispozici školní notebook, který slouží k ovládání projektorů, pouštění prezentací a jiným vyučovacím potřebám. Učitel nese za svůj notebook odpovědnost, jak ve škole, tak mimo ni.

Učitelé mají u notebooku administrátorská práva, mohou tedy instalovat všechny programy podle potřeb, nicméně přístup k školní síti mají pouze v prostorách školy (učebny, kabinet) při připojení přes UTP kabel. Není tedy možné, aby se neoprávněná osoba (např. při krádeži) dostala do školní sítě a napadla ji.

Tiskárny a scannery

Tiskárny ve škole nejsou veřejně přístupné studentům, kvůli možnému nezodpovědnému chování. O veřejných tiskárnách se nicméně uvažuje při zavedení jmenných účtů pro každého studenta.

Největší tiskárna, pro větší potřeby tisku, je umístěna v ředitelně. Dále jsou tiskárny přidávány do vybraných kabinetů učitelů.

Scannery jsou situovány v učebnách ICT a ředitelně.

Projektory a interaktivní tabule

Nyní je již ve zhruba polovině učeben k dispozici projektor, ke kterému se lze připojit pomocí již zmíněných učitelských notebooků. V odborných učebnách jsou umístěny interaktivní tabule, ke kterým se lze také připojit pomocí školních notebooků, stejně jako v případě projektorů.

Server a HW firewall

Škola vlastní dva servery, kde jeden slouží pouze jako záložní v případě výpadku primárního serveru. Primární server je značky Dell (model Dell PowerEdge T110 II), který je umístěný v místnosti, která má nejlepší podmínky pro umístění serveru. V místnosti je dobrá teplota, vlhkost a relativně bezprašné prostředí, takže slouží jako alternativa serverovny. Server primárně slouží k chodu informačního systému Bakaláři a správě účtů.

V případě výpadku elektrické energie je v místnosti umístěn UPS, který zajistí chod serveru, případně zajistí standartní vypnutí serveru.

Ve stejné místnosti je umístěn také hardwarový firewall k lepší síťové ochraně.

Místnost, kde je umístěn server, je vždy zamčený s přístup do místnosti má pouze správce IT. V místností je také protipožární ochrana a malé okno je chráněné mřížemi.

Obrázek 18: Server

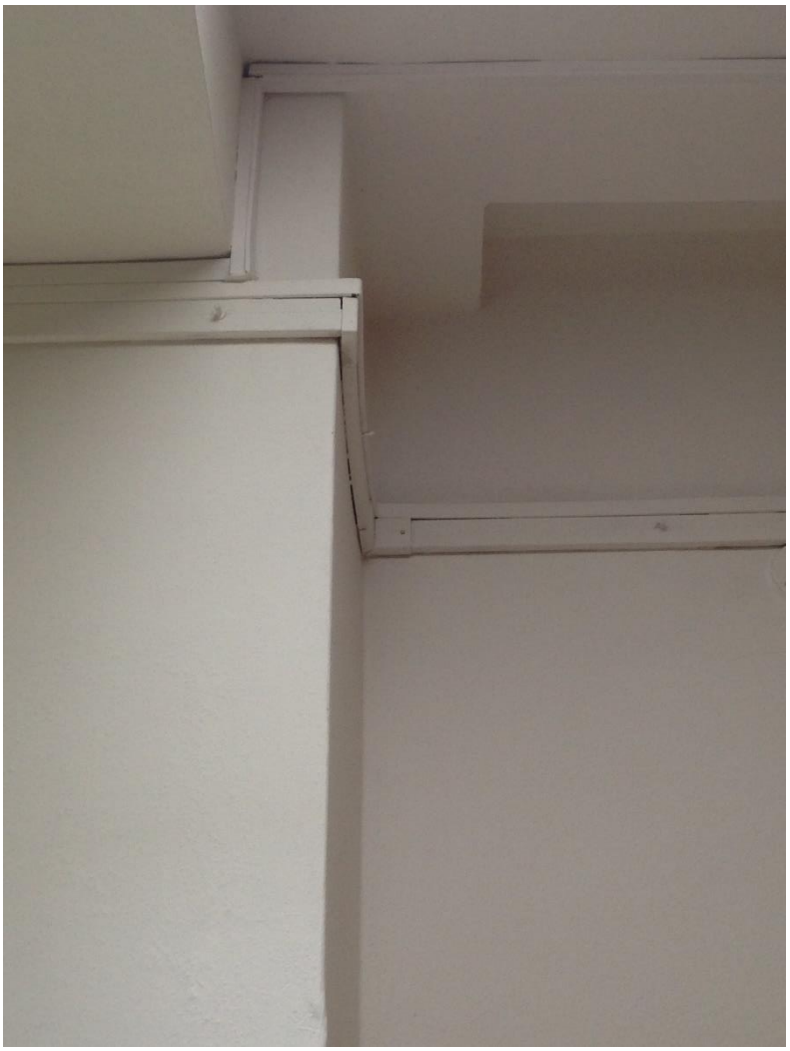
Síťová infrastruktura

Síťová infrastruktura prošla za svou historii řadou změn, převážně postupným přidávání kabeláže do částí školy, kde dříve kabeláž nebyla potřeba. Původní instalace počítačové sítě je stara 22 let a poslední změna proběhla před pěti lety, takže síť není v příliš dobrém stavu, včetně její dokumentace. Pomocí switchů je síť rozprostřena po všech částech budovy, většině učeben a kabinetů. Toto řešení se zavedlo z důvodu, že ve škole není zavedena wifi síť a učitelé by měli mít přístup k síti ze svých notebooků.

Kabeláž sítě je vedena v plastových lištách podél stropů, neboť v době, kdy byla škola stavěna, nebylo s datovou kabeláží počítáno. Kabeláž není jinak chráněna, nicméně díky výšce stropů není běžně přístupná. Teoretická rychlost sítě je 100Mbit/s.

Datové zásuvky v budově nejsou nijak chráněny, zároveň však nejsou veřejně dostupné a jsou instalovány pouze do míst, kde je využívají zaměstnanci (kabinet, vybrané učebny) nebo v učebnách ICT, kde mají žáci povolený vstup pouze s vyučujícím. Zásuvky, ke kterým jsou připojeny počítače na chodbách, jsou "napevno" zadělané skříní a žáci k nim nemají přístup. Tento způsob řešení je z již zmíněného důvodu, že ve škole není zabudovaná wifi, neboť počítačová síť není v optimálním stavu a rozšíření by stálo velké finanční prostředky. Dále také z bezpečnostních důvodu, aby nedošlo k odcizení notebooku a následnému připojení do školní sítě přes bezdrátovou síť.

Vedení školy se pokoušelo o zabudování wifi sítě po celé škole, nicméně se rozhodlo, že si nechá vytvořit projekt od externí firmy, která zajistí kompletní předělání síťové infrastruktury. Od projektu je požadováno, mimo jiné, vytvoření nove páteřní sítě s optickou kabeláží, wifi připojením a přenosovou rychlostí 10Gbit/s.



Obrázek 19: Žlaby pro kabeláž

2.3.2 Software

Informační systém

Škola využívá software Bakaláři, který se osvědčil ve většině škol České republiky. Software Bakaláři je využíván k evidenci žáků, zaměstnanců, školní matriky a rozvrhu hodin. Z důvodu nepřítomnosti wifi není využíván modul elektronické třídní knihy, díky problémovému zápisu, kdy by se v průběhu vyučování zapisovalo do papírové třídní knihy a až dodatečně opět přepisovalo do elektronické podoby. Elektronickou třídní knihu je plánováno začít používat po zavedení nové síťové infrastruktury. Přístup do systému mají učitelé, kteří mají svoje jmenné účty a správce je ředitel školy. Stejný způsob řešení je plánován i se zapisováním absencí a elektronického indexu.

Systém pro správu účetnictví je zaveden od společnosti Vema, a.s., kde správce je pouze účetní školy.

SW vybavení počítačů

Většina počítačů v ICT učebnách a v noteboocích učitelů jsou vybaveny operačním systémem Windows 7 Professional, případně Windows XP v počítačích na chodbě.

Každý počítač je vybaven kancelářským balíkem Windows Office a dalšími výukovými programy, především grafickými.

Počítače jsou vybaveny firewallem AVG s placenou verzí AVG Ultimate. Antivirová kontrola zařízení probíhá automaticky v pravidelných intervalech.

2.4 Fyzická bezpečnost objektu

Vstup do budovy je umožněn třemi vchody. První a zároveň hlavní vchod, je otevřen v době vyučování a je snímán kamerovým systémem. V době, kdy neprobíhá výuka, jsou dveře zamknuté čipem a centrálním klíčem. Klíče má k dispozici vedení školy a školník, který školu zpravidla ráno odemyká již zmíněným centrálním klíčem a přiložením čipu.

Obrázek 20: Přístupový systém

Další dveře jsou umístěny ze stejné strany školy a vedou přímo k ředitelně, nicméně dveře jsou většinu času zamknuty a přístup k nim mají pouze zaměstnanci s centrálním klíčem. Dveře jinak nejsou nijak hlídané a chráněné.

Třetí vstup je z opačné strany školy a vede do levého křídla školy. Dveře jsou stejně jak předchozí většinu času zamknuty a přístup k nim mají opět zaměstnanci s centrálním klíčem. Dveře jsou prosklené a nejsou nijak chráněné a zabezpečené. Kousek od třetího vchodu je postaveno parkoviště pro zaměstnance, které je hlídáno kamerovým systémem.

Škola využívá klidné lokality, kde útoky jako jsou krádeže nejsou obvyklé, tudíž o dodatečnou fyzickou bezpečnost škola neusiluje.

Obrázek 21: Třetí vchod

2.5 Kategorizace uživatelů a jejich práva

Pro stanovení pravomocí ve školní síti je využíváno služby MS Active directory, kde administrátor je IT správce školy. Uživatelé se dělí do čtyř skupin:

- Admin
- Supervizor
- IT učitelé
- Ostatní učitelé a zaměstnanci

Jak bylo zmíněno, roli admin má pouze IT správce školy a roli využívá k přidávání uživatelů do systému a jejich případné odebrání, přiřazování práv a jejich průběžné kontrole.

Roli supervizora mají dva lidé, jedná se o ředitele školy a správce IT učeben. Role není velmi využívaná a používá se pouze při absenci IT správce, neboť pravomoce jsou od admina velmi podobné. Při běžném přihlášení do systému používají oba dva svůj osobní profil, který má stejné pravomoce jako ostatní zaměstnanci, tedy velmi omezené.

IT učitelé mají roli, která je již omezená a nemohou účty přidávat, odebírat ani měnit práva ostatních účtu. Mohou však například resetovat heslo nebo zablokovat účet.

Poslední skupina má minimální práva, tudíž nemohou ani vidět ostatní uživatele ve skupině, ani cokoliv upravovat.

V současné době mají tedy svůj vlastní jmenný účet pouze zaměstnanci školy. U žáků se plánují zavádět jmenné účty pro žáky druhého stupně, nicméně zatím je to pouze plán a přesný čas zavedení neexistuje. Pro žáky nižšího stupně se jmenné účty zavádět neplánují.

2.6 Zavedená bezpečnost dat

Bezpečnost dat je řešená dvěma zálohami, kde jedna záloha je ukládána na lokální disk a druhá slouží jako offsite mimo školu.

Údaje o studentech jsou ukládány do informačního systému Bakaláři, takže základní bezpečnostní opatření jsou obsaženy v samotném IS. V systému jsou ukládány tyto údaje:

- Identifikační údaje
- Základní údaje o rodině
- Kontaktní údaje na zákonného zástupce
- Zdravotní údaje

Ukládané údaje o zaměstnancích:

- Identifikační údaje
- Zdravotní údaje a zdravotní pojišťovna
- Dosažená praxe a vzdělání
- Účetní údaje

Informace o studentech jsou tedy elektronicky ukládány a následně i zálohovány. Informace o zaměstnancích jsou v papírových kartotékách v ředitelně.

Jak již bylo zmíněno, učitelé dostávají k použití notebooky a mají volný přístup k instalaci všech aplikací, data jsou tedy čistě v jejich správě, včetně jejich zálohy.

Díky informačnímu systému Bakaláři, kde je šifrování dat řešeno. Další šifrování nicméně není zavedeno nijakým způsobem, stejně tak není využíván rozsáhlejší monitoring logů a sítě. Služba Active directory umožňuje sledovat pouze datum a čas úpravy jednotlivých účtů.

V případě reklamací, škola posílá počítače nebo notebooky do servisu bez namontovaných harddisků, aby nedocházelo k jejich zneužití.

2.7 Analýza bezpečnosti dat dle normy ISO/IEC 27001

V této části budou napsána analýza vybraných a relevantních částí, které jsou definovány normou ISO/IEC 27001, nebyly sepsány v předchozích částech anebo jsou doplněny. Jednotlivé body jsou dány v příloze A normy ISO/IEC 27001:2014.

2.7.1 A.5 Bezpečnostní politika

Bezpečnostní politiku tvoří směrnice a pravidla, případně zvyklosti, které určují řízení, ochranu a distribuci aktiv vedoucí k bezpečnosti informací.

Dokument nebo směrnice, jak určuje norma, není nijak zaveden ani udržován. O bezpečnostní politice se ve škole ví a jsou známá a z těch mohou vycházet jednotlivé opatření, nicméně tyto informace nejsou sepsány.

Z výše uvedeného tedy vyplívá, že ve škole nejsou zavedeny ani dokumenty o změnách a přezkoumání změn v politice bezpečnosti.

2.7.2 A.6 Organizace bezpečnosti

Ve škole jsou stanoveny úrovně uživatelů, kdy jednotlivé skupiny mají přiřazená odpovídající práva ve školní síti, nicméně tyto informace nejsou nijak dokumentovány a jejich detailní rozsah ví pouze správce IT.

Odpovědnost informační bezpečnosti není sepsána, jsou dána pouze pravidla, kdy např. zaměstnanci mají odpovědnost za svoje notebooky, ale v případě ztráty není tato zodpovědnost nijak postihována a hmotná odpovědnost připadá na školu.

Příloha A.6 obsahuje také část týkající se mobilních zařízení, ale ty se ve škole nevyužívají, právě i díky znemožněnému přístupu do školní sítě ze vzdáleného místa.

2.7.3 A.7 Bezpečnost lidských zdrojů

Bezpečnost lidských zdrojů se dělí na tři části:

A.7.1 Před vznikem pracovního vztahu

Škola odpovídá za své zaměstnance po podepsání pracovní smlouvy. Zaměstnanec musí doložit identifikační údaje, doklad o dosaženém vzdělání a zdravotní stav. Dokumentace existuje v podobě pracovní smlouvy, která je vytvořena na základě pracovního řádu ČR.

Zaměstnanec dostane po podepsání smlouvy vlastní jmenný účet do systému a k němu přiřazené odpovídající pravomoce. Informace v podobě bezpečnosti informací nejsou dokumentovány.

A.7.2 Během pracovního vztahu

Zaměstnanci jsou vždy na začátku školního roku školeni ohledně IT bezpečnosti, ale školení není nijak normované a zdokumentované.

A.7.3 Ukončení nebo změna pracovního vztahu

Po ukončení pracovního vztahu, které je konáno dle pracovního řádu ČR, jsou zaměstnanci odebrány všechny přístupy do školy a účet ze školního systému. Všechny neaktivní účty jsou mazány jednou ročně během školních prázdnin.

2.7.4 A 8 Řízení aktiv a odpovědnost

Dokumentace ohledně řízení aktiv, tj. zdokumentovaná odpovědnost osob za jednotlivé přístroje, oprávnění je používat nebo např. přenášet nejsou dokumentovaná dle platných norem, nicméně seznamy zařízení a jejich případných (ne nutně) majitelů je vytvořen.

Likvidace elektroniky probíhá převozem do sběrných dvorů k ekologické likvidaci.

Klasifikace informací je seřazena dle normy na veřejné (informace dostupné na webu školy), interní (známky studentů, formuláře, metodiky) a utajené (identifikační údaje studentů a zaměstnanců, mzdy)

2.7.5 A 9 Řízení přístupu

Problematika je již popsána v kapitole 2.5.

2.7.6 A 10 Kryptografie

Kryptografické metody nejsou ve škole zavedeny

2.7.7 A 11 Fyzická bezpečnost

Problematika byla popsána v kapitole 2.4.

2.7.8 A 12 Bezpečnost provozu

Programy v učebnách i notebooky učitelů jsou chráněny placeným antivirem od AVG, kde aktualizace programu jsou řízené aplikací a skenování celého zařízení je pravidelně naplánováno. Problémem může být, že skenování zařízení může nastat během výuky a student má pravomoce sken vypnout a odložit ho tak o další cyklus.

Škola využívá HW firewall využívající paketové filtrování.

Zálohování a monitoring je popsán v kapitole 2.6

2.7.9 A 13 Bezpečnost komunikace

Jak bylo zmíněno, počítačová sít je ve velmi špatném stavu a bylo již dvakrát rozšiřována, nicméně bez patřičné dokumentace a bez vzniku mapy sítě. Více informací o stavu počítačové sítě v kapitole 2.3.1.

Škola také nevyužívá digitálního podpisu.

2.7.10 A 14 Akvizice, vývoj a údržba

Všechny programy a informační systém Bakaláři jsou spravovány třetí stranou, takže škola se o provoz nestará.

2.7.11 A 15 Dodavatelské vztahy

Škola v případě nákupu většího množství elektroniky využívá zakázky z výběrového řízení, které podléhá zákonům ČR. Pro ostatní aktiva jsou dodavatelé smluvně vázáni na dobu určitou a všechny podmínky jsou sepsány v dodavatelské smlouvě.

2.7.12 A 16 Řízení incidentů bezpečnosti informací

Ve škole není zavedena žádná dokumentace nebo metodika, která by řešila případné postupy při řešení události nebo incidentů. Incidenty vždy řeší operativně správce IT.

2.7.13 A 17 Aspekty řízení kontinuity činností organizace z hlediska bezpečností informací

Škola nemá nijak řešenou a zavedenou kontinuitu bezpečnosti informací.
Redundanci je možné řešit náhradním serverem, který je k dispozici v serverovně, více popsáno v kapitole 2.3.1

2.7.14 A 18 Soulad s požadavky

Škola splňuje všechny zákonné požadavky a neporušuje žádnou normu trestního nebo občanského práva, zákonné nebo smluvní povinnosti a bezpečnostní požadavky.

2.8 Budování bezpečnostního povědomí – SAE

SAE není přímým způsobem ve škole řešeno, nicméně ve škole bývají zaměstnanci seznamováni se zacházením s informační technikou, jako jsou notebooky a další elektronické zařízení. V oblasti bezpečnosti dat však jsou seznámeni jen velice povrchně.

Žáci jsou seznamováni pravidelně každý rok o bezpečnosti chování v ICT učebnách, nicméně toto se zaměřuje spíše přímo na chování v učebnách, jako je zákaz jídla v učebnách, zákaz používání internetu na jiné než výukové potřeby.

Žáci v průběhu studia mají dva povinné předměty v ICT učebnách a jeden volitelný v devátých třídách. Výuka se v předmětech zaměřuje především na práci s grafickými programy, jako je Zoner photo studio a Gimp.

Studentům jsou v nepravidelných intervalech k dispozici přednášky, kde jsou poučování o kyberšikaně a bezpečném chování na sociálních sítích právě z pohledu kyberšikany.

3 VLASTNÍ NÁVRH

V části vlastního návrhu se vychází z části analýzy současného stavu, a tedy i z normy ISO/IEC 27001. V části bude přídán vlastní návrh k opatřením, které jsou v současnosti nejméně zabezpečené.

3.1 Analýza rizik

Navrhnuté opatření, která jsou popsána níže, by měla být založena na rizicích. V této části budou tedy rizika identifikována a k nim přiřazena hodnota, která určí pravděpodobnost a závažnost daného rizika.

Pro správné určení matice rizik je potřeba identifikovat aktiva, hrozby a vytvořit matici zranitelnosti. Na základě těchto informací, získáme vynásobením jednotlivých položek hodnotu, která je v matici rizik. Postup analýzy rizik je tvořen pomocí matice aktiv, hrozeb a zranitelností. (34)

3.1.1 Identifikace aktiv

V identifikaci aktiv k určení velikosti dopadu na jednotlivá aktiva, která jsou důležitá pro bezpečnost informací. Posouzení dopadu na aktiva jsou hodnocena dle současného stavu ve škole a dle mého uvážení, které vzniklo během analýzy školního prostředí a konzultacemi s odpovědnými osobami ve škole.

Tabulka 1: Identifikace aktiv

Název aktiva	Dopad
Server	3.5
Papírové smlouvy a dokumentace	5
Elektronické smlouvy	5
Síťová infrastruktura	4
Vybavení PC učeben	5
HW firewall	3
Zálohy dat	3
Notebooky učitelů	4

Hodnocení aktiv

Tabulka 2: Hodnocení aktiv

Hodnota	Dopad
3 - Střední	Malý nebo střední dopad pro školu. Dá se bez aktiva dočasně obejit
4 - Velká	Velký dopad pro školu
5 - Významná	Významný nebo velmi velký dopad pro školu

Hodnocení aktiv obsahuje stupnici pouze od 3 do 5 z důvodu, že ve škole jsou dopady nejníže právě na hodnotě tři, tedy malý nebo střední dopad pro školu.

3.1.2 Identifikace hrozeb

Identifikace hrozeb slouží k posouzení pravděpodobností vybraných hrozeb, které mají škodlivý dopad na vybraná aktiva v předchozí kapitole. Z tabulky lze vidět, že největší pravděpodobnost je v neoprávněném vstupu do školy, poruchy HW a neoprávněném použití zařízení uvnitř školy.

Tabulka 3:Identifikace hrozeb

Název hrozby	Pravděpodobnost
Krádež	2.5
Neoprávněný vstup do školy	4
Neoprávněný vstup v prostorách školy a neoprávněné použití zařízení	3.5
Nefunkční SW	3
Porucha HW	4
Výpadek elektřiny	2
Požár	1.5
Ztráta dat	3

Hodnocení hrozeb

Hodnocení hrozeb je stejné jak v předchozím případě, tedy dle mého uvážení na základě analýzy prostředí a konzultace s představiteli školy. Hodnocení hrozeb lze mít v různých intervalech, nicméně v tomto případě jsem zvolil interval 0-4, aby následná matice rizik byla v možném rozmezí 0-100.

Tabulka 4: Hodnocení hrozeb

Hodnota pravděpodobnosti	Pravděpodobnost
1	Velmi malá
2	Malá
3	Možná
4	Pravděpodobná

3.1.3 Matice zranitelnosti

Matice zranitelnosti slouží k posouzení zranitelnosti jednotlivých aktiv jednotlivými hrozbami. Tyto data jsou pak doplněna do tabulky a budou sloužit jako podklad pro následné vyplnění matice rizik. Pro výběr hrozeb a formát tabulky lze využít katalog, který je uvedený v normě ČSN ISO/IEC 27005 (nahrazená starší normou ČSN ISO/IEC TR 13335). Vypracovaná matice zranitelnosti je v tabulce 6.

3.1.4 Matice rizik

Matice rizik slouží k výpočtu míry rizika. Výsledek k jednotlivým buňkám tabulky získáme vynásobením hodnoty aktiva, pravděpodobnost hrozby a hodnoty z matice zranitelnosti. Výsledná hodnota udává míru rizika a ta je přiřazena k hranici pro nízkou, střední a vysokou hranici rizika. Zvolené intervaly jsou v tabulce 5 níže. Vypracovaná matice rizik je zobrazena v tabulce 7.

Klasifikace rizik

Tabulka klasifikace rizik udává, jak velké riziko, zobrazené v tabulce 7, představují jednotlivé hodnoty.

Tabulka 5: Klasifikace v matici rizik

Hranice	Velikost rizika
0-33,3	Malá
33,4-67,7	Střední
67,8-100	Velká

Tabulka 6: Matice zranitelnosti

	D	3.5	5	5	4	5	3	3	4
P	Riziko	Server	Papírové smlouvy a dokumenty	Elektronické smlouvy a dokumenty	Síťová infrastruktura	Vybavení PC učeben	HW firewall	Zálohy dat	Notebooky učitelů
2.5	Krádež	3	3	3	2	4	3	4	5
4	Neoprávněný vstup do školy	3	3	3	3	4	3	4	4
3.5	Neoprávněný vstup v prostorách školy a neoprávněné použití zařízení	4	4	4	3	4	3	4	5
3	Nefunkční SW	3	0	2	0	3	2	0	1
4	Porucha HW	4	0	3	3	4	3	1	1
2	Výpadek elektřiny	2	0	3	3	4	3	2	3
1.5	Požár	4	3	3	2	4	3	3	4
3	Ztráta dat	3	4	2	0	1	2	2	3
4	Neůmyslné zavinění	0	2	3	4	4	1	1	4

Tabulka 7: Matice rizik

Riziko	Server	Papírové smlouvy a dokumentace	Elektronické smlouvy	Síťová infrastruktura	Vybavení PC učeben	HW firewall	Zálohy dat	Notebooky učitelů
Krádež	26.25	37.5	37.5	20	50	22.5	30	50
Neoprávněný vstup do školy	42	60	60	48	80	36	48	64
Neoprávněný vstup v prostorách školy a neoprávněné použití zařízení	49	70	70	42	70	31.5	42	70
Nefunkční SW	31.5	0	30	0	45	18	0	12
Porucha HW	56	0	60	48	80	36	12	16
Výpadek elektřiny	14	0	30	24	40	18	12	24
Požár	21	22.5	22.5	12	30	13.5	13.5	24
Ztráta dat	31.5	60	30	0	15	18	18	36
Neúmyslné zavinění	0	40	60	64	80	12	12	64

3.1.5 Zhodnocení analýzy rizik

Ve vypracovaných tabulkách lze pozorovat nejvíce postižené oblasti, kde jsou největší rizika v oblasti bezpečnosti informací a že největší hrozby plynou z neoprávněného vstupu v prostorách školy a neoprávněném použití zařízení, neoprávněném vstupu do školy, krádeže a neúmyslného zavinění, takže v návrhu opatření je dobré se zaměřit hlavně na fyzickou bezpečnost a školení uživatelů (SAE).

3.2 Návrhy opatření dle normy ISO/IEC 27001

V této části budou vypsány bezpečnostní opatření dle normy ISO/IEC 27001, které jsou vhodné pro zavedení do prostředí základní školy.

3.2.1 A.5 Bezpečnostní politika

Pro umožnění zavedení ISMS ve škole je třeba mít potvrzení od vedení školy o realizaci a podporu ISMS. Ve škole bude zavedena dokumentace, kde budou definovány politiky pro bezpečnost informací a bude vytvořena pozice, popřípadě upravit stávající pozici, která se bude dokumentací a správou ISMS politik zabývat.

Cílem tohoto dokumentu je následující:

- Stanovení záměrů a cílů bezpečnosti informací
- Stanovení odpovědnosti (za důvěrnost, dostupnost, integrita)
- Stanovení zlepšování procesů dle PDCA cyklu
- Zajištění školení v oblastní bezpečnosti informací pro všechny zaměstnance a žáky základní školy
- Soulad s legislativou ČR, případně EU

Zavedení bezpečnosti informací ve škole a její dokumentace je také znak toho, že škola dbá jak na bezpečnost informací, tak na bezpečnost ve škole obecně.

Norma ISO/IEC 27001 ukládá, jaké body kvalitní bezpečnostní politika musí dodržovat:

- Odpovídá účelu organizace
- Zahrnuje cíle bezpečnosti informací nebo poskytuje rámec pro nastavení bezpečnosti informací
- Zahrnuje závazek pro splnění příslušných požadavků, které se týkají bezpečnosti informací

- Zahrnuje závazek k neustálému zlepšování ISMS
- Politika bezpečnosti informací musí být:
    - K dispozici jako zdokumentované informace
    - Sdílení pouze v rámci organizace
    - K dispozici všem zúčastněným stranám

Druhá část bodu A.5 se zabývá přezkoumáváním politik pro bezpečnost informací. Je tedy nutné, aby dokumentace, zmíněna v první části, byla pravidelně revidována a doplňována o nové a aktuální informace. V případě zjištění nedostatků, je nutné, aby pověřená osoba vypracovala novou dokumentaci, nebo upravila původní.

3.2.2 A.6 Organizace informační bezpečnosti

Ve škole budou zavedeny a definovány role, které zodpovídají za bezpečnost informací a za její platnou dokumentaci. V případě základní školy bych doporučoval alespoň jednu takovou osobu, která by měla zodpovědnost za následující:

- Bezpečnost informací
- Vytvoření a správa bezpečnostní dokumentace
- Zajištění školení pro zaměstnance a studenty, případně dohled na zajištění studijního předmětu pro studenty, zabývající se informační a kybernetickou bezpečností
- Správa bezpečnostních události a hlášení incidentů NCKB
- Dohled nad bezpečností HW a SW v učebnách školy
- Dohled nad počítačovou sítí a její bezpečnost

Pozici je možné i řešit přes externího pracovníka, nicméně tato možnost je mnohem dražší než najmutí, případně vyškolení stávajícího pracovníka.

V oblasti organizace je třeba stanovit také strukturu, kde bude jasné, komu se daný člověk zodpovídá a komu musí hlásit bezpečnostní incidenty. V bezpečnostní politice je tedy nutné mít zaznamenané procedury, politiky a kontaktní seznam, který specifikuje, koho je třeba kontaktovat v případě bezpečnostní události nebo incidentu.

3.2.3 A.7 Bezpečnost lidských zdrojů

Bezpečnost lidských zdrojů je momentálně řešená relativně dobře. Zaměstnanci mají jednou ročně (na začátku školního roku) školení ohledně bezpečnosti a údaje o studentech jsou uloženy v aplikaci Bakalář, kde je již zabudovaná bezpečnost. Bylo by vhodné doplnit školení zaměstnanců přímo při prvních dnech v zaměstnání, a to z důvodu, že zaměstnanec může nastoupit do pracovního poměru chvíli po novém roce, tudíž školení ho čeká až další rok.

V politice bezpečnosti informací musí být zahrnuty i informace o formě smluv se zaměstnanci a externími firmami:

- Každý zaměstnanec, který bude mít přístup k utajeným informacím musí podepsat dohodu o mlčenlivosti k nezveřejnění žádných z těchto informací během i po ukončení pracovní smlouvy
- Zaměstnanci budou předvedeny všechny práva a povinnosti týkající se ochrany bezpečnosti údajů
- Zaměstnanci bude seznámen s povinnostmi ohledně klasifikace informací a aktiv které jsou spojeny s informační bezpečností
- Zaměstnanec bude seznámen s povinnostmi a pravidly, které se týkají přenosu informací a aktiv mimo prostory organizace
- Zaměstnanec je seznámen s postihy v případě porušení požadavků informační bezpečnosti organizace

Informace o zaměstnancích existují pouze v papírové podobě, takže je vhodné údaje zdigitalizovat a nahrát na zabezpečená úložiště.

Při změně nebo ukončení pracovního poměru, jsou uživatelské účty mazány jednou ročně v době školních prázdnin. Neaktivní uživatelské účty je třeba mazat v co nejkratší době. Současný přístup umožňuje zneužití účtu osobou, která již není zaměstnancem, nicméně účet má stále aktivní do doby školních prázdnin.

Při ukončení pracovního poměru je zaměstnanec povinen odevzdat všechna aktiva, která dostal v době pracovního poměru, jako jsou všechny přístupy do školy a učeben a školní notebooky v případě učitelů.

3.2.4 A 8 Řízení aktiv a odpovědnost

V současné době existuje kompletní výpis aktiv ve škole, nicméně chybí jejich označení důležitosti z hlediska informační bezpečnosti pro zachování integrity, dostupnosti a důvěrnosti. Zároveň chybí přiřazení odpovědnosti za jednotlivá aktiva. Nyní je všechna odpovědnost přiřazena obecně na školu kromě učitelských notebooků, kde učitelé odpovídají za jejich ztrátu nebo odcizení. Je doporučeno tedy k seznamu aktiv přiřadit jejich důležitost a odpovědnou osobu u všech aktiv. Za kompletní seznam aktiv by byla zodpovědná osoba zmíněna v části A.6 Organizace bezpečnosti.

Při předávání aktiv zaměstnancům je potřeba mít zdokumentované a podepsané jak zaměstnancem, tak zodpovědnou osobou ve škole, jaká aktiva jsou předávána. Zaměstnanec musí také být plně seznámen s přebírající zodpovědností a seznámen s pravidly používání daného aktiva.

Jak bylo zmíněno v analýze, při reklamaci jsou v případě počítačů vyjmuty disky z bezpečnostních důvodů a při případné likvidaci jsou ekologicky zlikvidované v blízkém sběrném dvoře. V tomto případě je řízení aktiv v pořádku a není třeba zavedený postup měnit.

Klasifikace informací je ve škole řešena a je dělena na tři úrovně – veřejné, interní a utajené. Tento způsob řešení je považován jako dostatečný.

Jako příklad pro evidenci aktiv a jejich rizika jsou obsažena v příloze IV.

3.2.5 A 9 Řízení přístupu

Rozdělení uživatelů bylo popsáno již v analýze, jedná se tedy o skupiny Admin, Supervizor, IT učitelé, ostatní zaměstnanci a učitelé. Rozdělení uživatelů probíhá v MS Active Directory a jejich registrace a rušení je popsána v části A.7 Bezpečnost lidských zdrojů.

Žáci jmenné účty nemají zavedené a škola zamýšlí zavedení těchto účtu pro studenty druhého stupně. Jmenné účty by pro přihlášení do systému měli být obecně samozřejmostí, nicméně problém může nastat u prvních ročníků, kdy pro nové žáky může být uchovávání účtu a správa účtu problematická.

Pro základní školu navrhuji vytváření jmenných účtů pro žáky od čtvrtých tříd, kde mají za sebou již předměty s práci v IT učebnách a jsou tak s těmito informacemi dobře

seznámeni. Studenti nižších ročníků budou mít univerzální přístup s velmi omezenými pravomocemi.

Pro uživatele s vlastními notebooky a jmennými účty by měly být stanoveny pravidla pro správu těchto účtů:

- Heslo minimálně 8 znaků
- Povinnost komplexního hesla
- Expirace hesla a nutnost změnit heslo 1x ročně
- Nové heslo nesmí být žádné z předcházejících deseti použitých hesel
- Stanovení maximálního limitu pro změnu hesla – max. 1x ročně nebo požádat o změnu hesla ICT správce (odpovědná osoba)
- Zamknutí účtu po pátém neúspěšném pokusu o přihlášení
- Nastavení automatického uzamykání notebooku po neaktivitě 5 min

Pravomoce ke změně nebo resetování hesla má pouze pověřená osoba z kategorie Admin nebo Supervizor.

3.2.6 A 10 Kryptografie

Ve škole by mělo být zavedeno šifrování disků v počítačích a noteboocích učitelů pro případ jeho odcizení. Dále je třeba zavést šifrování záloh. Pro šifrování disků je k dispozici široká řada programů a nástrojů, jedním z nejznámějších a kvalitních je BitLocker, který je součástí většiny verzí MS Windows (Vista a novější)

Obrázek 22: Bitlocker (32)

I přes to, že data nejsou ve škole žádným způsobem šifrována, o bezpečnost informací je v tomhle směru dobře postaráno (znemožněný přístup do školní sítě mimo budovu, reklamace počítačů bez pevných disků a zálohy)

3.2.7 A 11 Fyzická bezpečnost

Tato kapitola je bude rozdělena do dvou částí dle normy 27001 – Zabezpečené oblasti a Bezpečnost zařízení

A.11.1 Zabezpečené oblasti

V analýze bylo popsáno, že do školy existují tři vstupy. Hlavní vstup je relativně dobře hlídaný, kde je zabudovaná kamera a po vyučování je na chodbě a u vstupu dohlížející, většinou jeden z učitelů. Podrobnější popis je popsán v analýze současného stavu. Z pohledu bezpečnosti je hlavní vstup dobře střežen a potencionálnímu útočníkovi nedává příliš příležitostí. V případě narušení hlavního a vedlejšího (viz. další odstavec) vstupu je upozorněna policie ČR, která zasáhne na místě a upozorní povolané zaměstnance a ředitele školy. V ranních hodinách, kdy jde do školy nejvíce osob, je navíc před školou pravidelně policista, který řídí bezpečnost dopravy, tudíž na situaci v okolí hlavního vstupu dohlíží.

Obrázek 23: Kamera při vstupu

K těmto bezpečnostním opatřením bych využil školních čipů studentů, které jsou již nyní používány ve školních jídelnách, aby byly žáci nuceni použít čip v případě, že přijdou do školy později. Návštěvy nebo studenti, kteří čip zapomenou, by byli nuceni použit komunikátor na dveřích a příchod ohlásit. Používat čipy v každém případě mi nepřipadá vhodné z důvodu velkého počtu studentů, kteří ráno vstupují do budovy a tento způsob by mohl být zneužíván tak, že by jeden žák byl schopen pustit více osob najednou.

Druhý vstup je většinu času zamčen a obsahuje alarm, nicméně chybí kamerový systém a pro vstup stačí klíč bez použití čipu, jako je v případě hlavního vstupu. Výhodou v době vyučování je, že prostředí u těchto dveří je velmi rušné a chodí tu velké množství zaměstnanců. Druhý vstup je také dobře zabezpečený, pouze by bylo vhodné přidat další kameru ke vstupu, která by mohla hlídat také jízdní kola, která jsou umístěna hned vedle tohoto vstupu.

Třetí vstup je nejméně zabezpečen, je umístěn v zadní části školy a nedisponuje žádnými většími ochrannými mechanismy. Skleněné dveře jsou zamčené a vedou do tělocvičen školy, které jsou dále propojeny s chodbou školy. Dveře se vždy zamykají a vstup je přes centrální klíč. Dveře, které jsou dále propojeny s chodbou jsou v době výuky otevřené a zamyká je učitel tělocviku vždy při odchodu ze školy. Vstup není přímo hlídán kamerovým systémem, ale je umístěn k blízkému parkovišti, nicméně útočník by byl schopen se ke dveřím dostat bez zpozorování.

Třetí vstup je tedy největší fyzickou slabinou a byl by vhodné dveře opatřit alespoň alarmem a původní dveře vyměnit za kvalitnější a vyrobeného z bezpečnějšího materiálu. Pro zachování maximální fyzické bezpečnosti by bylo vhodné mít u všech dveří povolen přístup nejen na klíč, ale také na čip, který se nyní používá pouze u hlavních dveří.

Uvnitř školy jsou všechny dveře na klíč, nicméně většina se nezamyká. Učebny, které se zamykají jsou s interaktivními tabulemi, případně jinou cennější technikou a klíče od těchto učeben mají všichni učitelé, kteří v učebně pravidelně vyučují. V tomto případě by bylo vhodné, aby byl o půjčených klíčích přehled, takže zavést zodpovědnou osobou, která bude zapůjčené klíče a osoby zapisovat.

Jak bylo zmíněno v analýze, škola má zavedenou serverovnu, která se však bere pouze jako místnost se serverem, kde je sice je relativně vhodné prostředí pro server (viz.

kapitola 2.3.1.), nicméně některé typické prvky, které jsou vhodné pro serverovnu zavedeny nejsou. Serverovna by měla mít zavedou následující ochranu:

- Bezprašné prostředí (splněno)
- Klimatizace
- Alternativní napájecí zdroj (splněno)
- Zabezpečení objektu (splněno)
- Evidence přístupu
- Zdvojená podlaha či strop
- Hasící přístroje (splněno)

Škola je postavena na vyvýšeném místě, tudíž není třeba dbát žádným způsobem na bezpečnost proti povodním a proti případnému požáru je ve škole protipožární ochrana a je zavedena požární poplachová směrnice.

A.11.2 Bezpečnost zařízení

Všechny počítače a přenosná elektronika by měla být v uzavíratelných a uzamykatelných skříních, aby se k nim nedostali žáci, kteří by mohli způsobit škody, např. o přestávkách. V určitých učebnách, převážně odborných, tyto skříně jsou, bylo by ale vhodné je nainstalovat do všech učeben, kde je elektronika používána.

Bezpečnost aktivních a pasivních prvků sítě je řešena v nedostupnosti zařízení pro studenty i zaměstnance. Lišty s kabeláží jsou vedeny na úrovní stropů a switche jsou v kabinetech učitelů nebo zamknuté v učebnách, takže ochrana síťových v prvků je řešena dostatečně.

Obrázek 24: Switch v ICT učebně

3.2.8 A 12 Bezpečnost provozu

V dokumentaci ohledně bezpečnostní politiky by mělo být zmíněno, resp. přidány pravidla ohledně volnosti žáků na internetu (zakázané pornografické stránky a stránky s nevhodným nebo škodlivým obsahem). Vlastní přenosné zařízení musí být před otevřením automaticky otestované nainstalovaným antivirem, to slouží jako prevence před infikovanými soubory na přenosném disku a následném možném poškození počítače nebo sítě.

Soupis pravidel pro bezpečnost proti malwaru:

- Zákaz použití neautorizovaného softwaru
- Prevence a detekce podezřelých webových stránek
- Instalace pravidelných updatů
- Využití principu oddělených sítí (viz. A 13)
- Snížení zranitelnosti (SAE)

Všechny tyto pravidla musí být sepsána a všichni uživatelé s nimi musí být obeznámeni. Ochrana školních počítačů pro studenty je dostatečná s placeným AVG antivirem a zabudovaným HW firewallem. Počítače jsou vybaveny operačním systémem Windows 7, které jsou automaticky aktualizované k nejnovější verzi. Počítače na chodbách mají nainstalovaný operační systém Windows XP, na který již společnost Microsoft nevydává bezpečnostní záplaty a aktualizace, je tedy vhodné přejít na novější operační systém, z dlouhodobého hlediska ideálně na Windows 10.

Jak bylo zmíněno v analýze, forma zálohování je řešena velmi kvalitně a není třeba tento způsob měnit – jedna záloha na disk a jedna záloha offsite.

Forma zálohování je řešena zálohou na disk a jednou zálohou offsite. Počet záloh je tedy dostačující, ale je třeba nastavit následující pravidla pro zálohování:

- Nastavení pravidelnosti záloh
    - Rozhodnutí, jaká data zálohovat
    - Nastavení pravidelné frekvence záloh
    - Nastavení přístupu k zálohám
    - Počet uložených záloh
- Kvalitní fyzická ochrana záloh
- Pravidelné testování záloh dat
- Šifrování záloh

Provoz na síti není v současné době nijak monitorován. Služba Active directory obsahuje monitoring v oblasti účtu (zakládání účtu, změna hesel apod.). Jako nástavbu k Active directory lze využít kompatibilní službu Splunk, který je schopen analýzy sítě a ukládat je do log souborů, zaznamenává vytížení sítě, vytváření pravidelných reportů a je uživatelsky přívětivý.

3.2.9 A 13 Bezpečnost komunikace

V této části je důležitá část oddělených sítí, kdy je třeba, aby byly rozděleny sítě pro studenty a pro zaměstnance. To pro zamezení, aby se studenti v učebnách nebo na volných počítačích na chodbě nedostali do školní sítě. Síť pro studenty by měla mít razantně větší míru blokovaných škodlivých stránek.

Tato problematika bude řešena v samostatném projektu navržení síťové infrastruktury, která bude vytvářena externí organizací.

3.2.10 A 14 Akvizice, vývoj a údržba

Škola žádný software nevytváří a o vše se starají třetí strany.

3.2.11 A 15 Dodavatelské vztahy

Dodavatelské vztahy jsou řešeny vždy dodavatelskou smlouvou. V tomto případě je nutné myslet na fakt, že v případě, kdy neseme informace nebo aktiva mimo školní prostředí, je třeba dbát na ochranu informací alespoň ve stejné míře. Pro splnění normy 27001 je třeba u dodavatelů dodržovat následující body:

- Dodavatelé mají přístup pouze k datům, ke kterým jsou předem autorizovány
- Dodavatelé jsou spravování, kontrolování a monitorováni k určitému datu
- Dodavatelé mají zabudované vlastní bezpečnostní politiky a procedury
- Dodavatelé pouze dodávají takové služby, které jsou od nich očekávány a služby nijak neohrozí organizaci nebo ji nevystaví riziku.

3.2.12 A 16 Řízení incidentů bezpečnosti informací

Jak bylo zmíněno na začátku vlastního návrhu, je třeba mít pověřeného pracovníka (Manažer informační bezpečnosti), který se bude starat o bezpečnostní události a případné incidenty hlásit NCKB.

3.2.13 A 17 Aspekty řízení kontinuity činností organizace z hlediska bezpečností informací

Škola by měla mít zdokumentovaný postup v případě, že nastane bezpečnostní incident a tento dokument pravidelně kontrolovat, případně upravovat. Více bylo zmíněno v bodu A.5 Bezpečnostní politika.

Redundance je řešena náhradním serverem, který je schopen provozu v případě výpadku primárního serveru a v případě výpadku energie, je k dispozici UPS, který je schopen udržet server v provozu po dobu bezpečného vypnutí a uložení všech dat.

3.2.14 A 18 Soulad s požadavky

Škola splňuje všechny zákonné požadavky, a tudíž tu není potřeba vlastního návrhu.

3.3 Budování bezpečnostního povědomí – SAE

Důvodem pro zavádění nebo budování bezpečnostního povědomí nejen ve školách, ale obecně v organizacích, je narůstající množství elektroniky, která se stala každodenní částí života. Bezpečnostní povědomí o informační bezpečnosti by mělo mít za následek zautomatizování právě bezpečného chování.

Ve škole bych doporučil zavedení předmětu zabývající se tématikou bezpečnosti, aby žáci získali alespoň obecné povědomí už od mala a byly obezřetní svým chováním na internetu a s elektronikou. Informace ohledně bezpečnosti informací by měli být prezentovány nejen formou výuky, ale i věšením letáků (inspirací pro letáky může být příloha D normy NIST 800-50), organizování seminářů a přednášek nebo exkurzemi do institutů zabývající se bezpečností, tematickými spořiči obrazovek, nebo např. dny bezpečnosti. Povědomí by přineslo dětem lepší znalost obrany, principy bezpečného chování a ochranu před dnes častými útoky jako je ransomware. V případě, že ve školním harmonogramu by nebylo na samostatný předmět volno, je možné zavést také online kurz (např. e-learning), kde mohou být žákům poskytovány materiály a do stanoveného data musí být odevzdaný test.

V zmíněným propagačních materiálech by měly být zmíněny následující základní body, které by žáci měli mít stále na paměti:

- Používat silné heslo a nikde heslo nešířit
- Heslo neschovávat na papírku vedle počítače, nalepené na skříni atd.
- Heslo pravidelně měnit
- Nesdílet osobní informace online
- Neotevírat neznámé přílohy v mailech
- Používat osvědčeny firewall
- Používat antivir
- Záloha dat
- V případě podezřelých událostí okamžitě hlásit dospělé nebo odpovědné osobě
- V případě odchodu od pracoviště nenechávat PC zapnutý

Jako příklad pro leták je uveden v příloze V.

Školení učitelů a zaměstnanců je ve škole zavedeno, nicméně danému školení by bylo dobré přidat na četnosti a vykonáváno externí organizací. Školení by mělo být zakončené testem, aby bylo dokázáno, že zaměstnanec rozumí problematice. To z důvodu, že dnes již běžně učitelé pracují s osobními údaji studentů. Tato část školení by měla být prováděna dle normy nebo určité metodiky. Norma zabývající se SAE může být normy a metodiky:

- **NIST 800-50** Building an Information Technology Security Awareness and Training Program,
- **NIST 800-16** - Information Technology Security Training Requirements
- **NIST SP 500-172** - Computer Security Training Guidelines
- **PCI DSS** (PCI Data Security Standard) - Security Awareness Program Special Interest Group

Ve škole by také měl být zaveden, resp. vyškolen zaměstnanec s certifikací dle ISO 27001 – Manažer informační bezpečnosti. V České republice toto školení poskytuje společnost CIS za poplatek 25 000,- Kč, cena je včetně zkoušky a certifikátu. Kurzy probíhají alespoň třikrát ročně, tudíž termín si lze stanovit s dostatečným předstihem a ve vhodném termínu. Kurz obsahuje tři moduly, které lze navštěvovat nezávisle na sobě:

- Norma ISO 27001 / ISO 27002
- Psychologické základy pro manažera IS
- Právní základy

Zvyšování bezpečnostního povědomí by tedy bylo děleno na tří úrovně, aby se každá skupina vzdělávala pouze v oblastech, které budou užitečné, a nikoliv přidávající zbytečně starosti:

- Školení žáků
- Školení zaměstnanců
- Školení bezpečnostního manažera

Příklad tvorby SAE programu lze najít v příloze II.

Předtím, než bude SAE program vytvořen, je dobré, aby účastníci programu vyplnili dotazník, které budou tvořit reprezentativní vzorec a ten ukáže, na jaké úrovni jsou

znalosti účastníků ohledně bezpečnosti informací. Vzorem pro takový typ dotazníku může být příloha A v normě NIST 800-50 (SAMPLE NEEDS ASSESSMENT INTERVIEW AND QUESTIONNAIRE). Příklad pro školu je v příloze III.

3.4 Ekonomické zhodnocení

V poslední části vlastního návrhu je třeba uvést předpokládanou částku, kterou musí být škola ochotna zaplatit. V tabulce není uvedeno budování nové síťové infrastruktury, která bude řešena v budoucnu, pravděpodobně v letech 2018/2019 a bude řešena samostatným projektem.

Celková výše nákladů na ISMS činí přibližně 162 200 Kč, kde největší položka se týká fyzické bezpečnosti, konkrétně úpravu ochrany a výměna dveří. Bez této položky by celková cena byla 95 500 Kč.

Cena bezpečnostního manažera je počítána z předem dané sazby společnosti CIS 25 000 Kč. Tvorba bezpečnostních politik je počítána z předpokládané hodinové sazby pracovníka 350kč a doby tvorby politik zhruba 55 hodin. Fyzická bezpečnost je rozdělena na tři části, kde ceny jednotlivých částí jsou doporučené z vybraných obchodů. Dvoukřídlé bezpečnostní dveře Adlo v hodnotě zhruba 50 000 Kč, kamerový systém D-Link v ceně 5 200 Kč za kus a alarm iGet Security M2B v hodnotě 3 000 Kč. Cena instalace fyzické bezpečnosti je odhadnuta na 3 500Kč.

Přístupový systém do serverovnu byl vybrán od společnosti 2N, která již škola používá pro hlavní vstup do budovy a jeho cena je 8 000 Kč. Klimatizace Guzzanti, která se prodává včetně interní jednotky za 15 000 Kč a zdvojený strop za 10 000 včetně práce. Instalace za jednotlivé položky (kromě instalace zdvojeného stropu) byla odhadnuta na 2 500 Kč.

Jednotlivé položky mohou být obměněny různými výrobci, kteří se liší kvalitou i cenou, proto jsou ceny uváděny pouze jako předpokládaná částka, kolem které se dané ceny položek pohybují.

I když se cena může zdát na první pohled vysoká, je to cena za ochranu studentů, zaměstnanců a všech dat školy, které mohou být zneužita a která by v konečném důsledku byla mnohem větší a dražší.

Tabulka 8: Rozpočet

Opatření	Cena (Kč) včetně DPH
Školení bezpečnostního manažera	25000
Tvorba bezpečnostních politik	20000
Fyzická bezpečnost	64700
Bezpečnostní dveře	50000
Kamerový systém	10200
Alarm	3000
Instalace	3500
Serverovna	34500
Přístupový systém	8000
Klimatizace	15000
Zdvojený strop	10000
Instalace	2500
Cena za vytvoření plánu pro návrh bezpečnostního řešení	15000

Cena celkem	160200

ZÁVĚR

V diplomové práci bylo dáno za cíl vytvoření bezpečnostních opatření, která jsou navržena na základě norem ISO/IEC 27000 a analýzy současného stavu. Současný stav byl zpracován dle veřejně dostupných informací a konzultací s klíčovými osobami ve škole.

Práce je rozdělena do tří částí, z toho první část jsou teoretická východiska. V té jsou popsány základní informace o informační bezpečnosti, bezpečnosti ICT a ISMS a jeho postupy zavádění.

Druhá část obsahuje analýzu současného stavu, tedy představení organizace, ICT vybavení, které je relevantní k informační bezpečnosti a současný stav zabezpečení informační bezpečnosti.

Třetí a zároveň poslední část je samotné navrhnutí bezpečnostních opatření na základě přílohy A v normě ISO/IEC 27001, navrhnutí zavedení bezpečnostního povědomí a finální ekonomické zhodnocení projektu.

Cíle práce jsou uvedené v úvodu jsou tedy splněny a po realizování projektu by měly být informace velmi dobře zabezpečené.

SEZNAM POUŽÍTÉ LITERATURY

1) ONDRÁK, Viktor, Petr SEDLÁK a Vladimír MAZÁLEK. *Problematika ISMS v manažerské informatice*. Brno: Akademické nakladatelství CERM, 2013. ISBN 978-80-7204-872-4.
2) DOSEDĚL, Tomáš. *Počítačová bezpečnost a ochrana dat*. Brno: Computer Press, 2004. ISBN 80-251-0106-1.
3) MLÝNEK, Jaroslav. *Zabezpečení obchodních informací*. Brno: Computer Press, 2007. ISBN 978-80-251-1511-4.
4) Důvěrnost-Integrita-Dostupnost. *Clever and Smart* [online]. 2008 [cit. 2017-05-13]. Dostupné z: http://www.cleverandsmart.cz/duvernost-integrita-dostupnost/
5) Infosec. *Tech Target* [online]. 2016 [cit. 2017-03-05]. Dostupné z: http://searchsecurity.techtarget.com/definition/information-security-infosec
6) Technické normy ČSN. *Technické normy* [online]. 2008 [cit. 2017-03-05]. Dostupné z: https://www.technickenormy.cz/tridy-norem-csn/
7) ISO members. *ISO* [online]. [cit. 2017-03-05]. Dostupné z: https://www.iso.org/members.html
8) ISO logo. *DWG logo* [online]. [cit. 2017-03-05]. Dostupné z: https://dwglogo.com/iso-logo/
9) About the IEC. *IEC* [online]. 2017 [cit. 2017-03-09]. Dostupné z: http://www.iec.ch/about/
10) O úřadu. *UNMZ* [online]. 2017 [cit. 2017-03-09]. Dostupné z: http://www.unmz.cz/urad/unmz
11) ISO/IEC 27001. *ISO 27001* [online]. 2017 [cit. 2017-03-09]. Dostupné z: http://www.iso27000.cz/rac/homepage.nsf/CZ/27001
12) PDCA. *Réfugio* [online]. 2016 [cit. 2017-03-09]. Dostupné z: http://refugioea.com/2016/03/22/gestao-ambiental-x-sistema-de-gestao-ambiental-e-so-uma-questao-de-certificacao/
13) PDCA. *PDCAHOME* [online]. 2017 [cit. 2017-03-09]. Dostupné z: http://pdcahome.com/english/267/pdca-cycle-continuous-improvement/
14) PDCA. *Vimeo* [online]. 2017 [cit. 2017-03-10]. Dostupné z: https://vimeo.com/144252898

15) PDCA. *CSN* [online]. 2006 [cit. 2017-03-10]. Dostupné z: http://csnonlinefirmy.unmz.cz/html_nahledy/36/76533/76533_nahled.htm
16) PROGRAMY ZVYŠOVÁNÍ BEZPEČNOSTNÍHO POVĚDOMÍ A ŠKOLENÍ. *Krucek Cyber Security Center* [online]. [cit. 2017-03-10]. Dostupné z: http://www.krucek.cz/cz/programy-zvysovani-bezpecnostniho-povedomi-a-skoleni-86011/
17) NCKB. *GOVCERT* [online]. [cit. 2017-03-10]. Dostupné z: https://www.govcert.cz/
18) SOSINSKY, B. *Mistrovství - počítačové sítě: Vše, co potřebujete vědět o správě sítí*. 1. vydání. Brno: Computer Press, 2011. ISBN 978-80-251-3363-7.
19) Šifrování dat. *Bezpečný internet* [online]. 2016 [cit. 2017-03-10]. Dostupné z: http://www.bezpecnyinternet.cz/pokrocily/ochrana-dat/sifrovani-dat.aspx
20) SEDLÁK, P Management bezpečnosti fyzické vrstvy [přednáška]. Brno: Workshop Služby a kvalita služeb, 27.11.2013.
21) Blokátory konektorů. *Conrad* [online]. [cit. 2017-04-01]. Dostupné z: https://www.conrad.cz/lan-blokatory-konektoru-rj45-renkforce-rf-lanblocker-01.k1487674#
22) Do you need an IDS or IPS, or both? *Tech Target* [online]. [cit. 2017-04-01]. Dostupné z: http://searchsecurity.techtarget.com/Do-you-need-an-IDS-or-IPS-or-both
23) Systémy prevence průniků (1) – jen detekovat nestačí. *Svět sítí* [online]. 2007 [cit. 2017-04-01]. Dostupné z: http://www.svetsiti.cz/clanek.asp?cid=Systemy-prevence-pruniku-1--jen-detekovat-nestaci-5112007
24) Introducing IDS and IPS. *Infosec Primer* [online]. 2013 [cit. 2017-04-01]. Dostupné z: https://infosecprimer.wordpress.com/2013/07/09/introducing-ids-and-ips/
25) What is VPN? *Whatismyipadress* [online]. [cit. 2017-04-01]. Dostupné z: http://whatismyipaddress.com/vpn
26) How VPNs Work. *How stuff works* [online]. [cit. 2017-04-01]. Dostupné z: http://computer.howstuffworks.com/vpn4.htm
27) ITIL® Demand Management. *BMC* [online]. [cit. 2017-04-01]. Dostupné z: http://www.bmc.com/guides/itil-demand-management.html

28) Updated Ideas On Straightforward Programs In Define Cloud Computing. *Copperhead* [online]. 2016 [cit. 2017-04-01]. Dostupné z: https://www.copperhead-brewing.com/tag/cloud-computing/
29) ITSM & ITIL®. *Best practice* [online]. [cit. 2017-05-13]. Dostupné z: https://www.bestpractice.cz/cs/Home.alej
30) Zákon o kybernetické bezpečnosti. *Národní bezpečnostní úřad* [online]. 2014 [cit. 2017-05-14]. Dostupné z: https://www.nbu.cz/download/pravni-predpisy/container-nodeid-1347/zkb-181-2014-sb.pdf
31) SEDLÁK, P Bezpečnost informací akademické/univerzitní prostředí [přednáška]. Brno: Bezpečnost informací, 3.11.2014.
32) Bitlocker. *MYU Computer* [online]. [cit. 2017-05-15]. Dostupné z: http://www.muycomputer.com/2015/12/17/bitlocker-en-windows-10/
33) NIST SPECIAL PUBLICATION 800-50. *COMPUTER SECURITY: Building an Information Technology Security Awareness and Training Program*. Washington, DC: National Institute of Standards and Technology, 2003.
34) Procesy. *BPM Projekt* [online]. [cit. 2017-05-15]. Dostupné z: http://bpm-tema.blogspot.cz/2007/11/ppadov-studie-analzy-rizik-informan.html

SEZNAM OBRÁZKŮ

SEZNAM TABULEK

SEZNAM PŘÍLOH

Příloha I

Bezpečnostní politika

Vzhledem ke stále zvyšujícímu nebezpečí nejen informační bezpečnosti, škola se rozhodla pro zavedení systému řízení bezpečnosti informací neboli ISMS. ISMS poskytne návod pro dostatečné zabezpečení všech informací a studentů zároveň.

Stanovení záměrů a cílů bezpečnosti informací

Škola si je vědoma závazků plynoucí z implementace ISMS a zavazuje se k plné podpoře implementace. Škola tak bude dbát na zajištění ochrany informací z pohledu integrity, důvěrnosti a dostupnosti. Dále bude podporovat úpravy v procesech, pokud bude nutno, jejich postupné vylepšování a pravidelné kontrolování.

Stanovení odpovědnosti (důvěrnost, dostupnost, integrita)

Zaměstnanci a žáci školy jsou informování a poučení o bezpečnosti informací a odpovědnosti za svoje chování v oblasti informační bezpečnosti. Zároveň se škola bude snažit o motivaci tuto zodpovědnost dodržovat a zároveň bude ochotná poskytovat všem relevantním osobám informace.

Stanovení zlepšování procesů dle PDCA cyklu

Škola se zavazuje k pravidelným kontrolám a zlepšování procesů zajišťující bezpečnost informací. Všechny procesy jsou kontrolovány dle PDCA cyklu a obsahují kontrolu všech důležitých informací školy.

Zajištění školení v oblastní bezpečnosti informací pro všechny zaměstnance a žáky základní školy

Škola zajistí pravidelné školení všem zaměstnancům a žákům potřebné školení pro znalost a chování z pohledu ICT bezpečnosti a bezpečnosti informací.

Soulad s legislativou ČR, případně EU

Všechny činnosti prováděné v rámci implementace bezpečnosti informací jsou v souladu se všemi zákony ČR a EU, případně dalšími relevantními smlouvami a požadavky.

……...……

Příloha II
SAE program (dle přílohy D normy NIST 800-50)

Informace o programu

Program SAE slouží ke zvyšování nebo budování bezpečnostního povědomí, které má za cíl zautomatizovat bezpečné chování na internetu a v oblasti informační bezpečnosti a předcházet tak bezpečnostním incidentům.

Povědomí

- Vybraní zaměstnanci a žáci, kteří budou SAE program vykonávat
- Stanovení aktivit a času školení
- Rozpis jednotlivých školení
- Revize materiálů a školících metod

Vzdělávání / trénink

Role 1: Žáci

Školení pro žáky je tvořeno formou propagujících materiálů a organizováním seminářů. Forma studia je tvořena vytvořením studijního předmětu zaměřující se na ICT bezpečnost

- Výuka dané problematiky
- Samostatné úkoly
- Testy v průběhu studijního předmětu
- Vyhodnocení testů na základě předem daných kritérií

Role 2: Zaměstnanci

- Výuka dané problematiky
- Samostatné úkoly
- Aktivity zaměřené na bezpečnost informací
- Stanovení testu
- Vyhodnocení testu na základě předem daných kritérií

Role 3: Systémový administrátor

- Výuka dané problematiky
- Samostatné úkoly
- Aktivity zaměřené na bezpečnost informací
- Stanovení testu
- Vyhodnocení testu na základě předem daných kritérií

Profesní certifikace

V případě školy se jedná o certifikace pouze role 3 – Systémový administrátor od externí organizace CIS

- Výuka dané problematiky
- Samostatné úkoly
- Aktivity zaměřené na bezpečnost informací
- Stanovení testu
- Vyhodnocení testu na základě předem daných kritérií

Příloha III

SAE dotazník (dle přílohy A normy NIST 800-50)

Pracovní pozice: _____ Datum: _____

Popis práce: _____

Tento dotazník je vytvořen ke zjištění znalostí, schopností a zkušeností pro používání a správu informačního systému, sítě a ke zjištění znalostí ohledně bezpečnosti informací. Dotazník pomůže porozumět vašemu současnému stylu práce ve zmíněných oblastech a ke zjištění, jaké oblasti by bylo dobré zlepšit a jaký typ školení by byl nejvíce vyhovující pro vaši současnou situaci. Dotazník zabere nejvýše 20 minut času ke kompletnímu vyplnění.

Část 1: Současné postavení

1. Je v současné době vaše pracovní náplň systémového správce? ANO NE

   1.a. Pokud ano, jedná se o práci na plný úvazek? ANO NE

   1.b. Pokud se jedná o částečný úvazek, kolik procent času práci věnujete?
   _____%

2. Jak dlouho pracujete jako systémový administrátor? _____
3. Podstoupil(a) jste někdy formální školení na pozici systémový administrátor?
   ANO NE
   3.a. Pokud ano, upřesněte:
   _____
4. Podstoupil(a) jste někdy školení v oblasti systémové bezpečnosti?
   ANO NE
   4.a. Pokud ano, upřesněte:
   _____
5. Napište, kolik let studia máte v daném oboru vystudováno: _____
6. Na kolika seminářích nebo konferencích jste se účastnil(a) v posledních dvou letech? Pokud ano, upřesněte:
   _____

7. Čtete časopisy nebo různé články ohledně ICT/bezpečnosti/PC sítí?

   ANO NE

Část 2: Současné schopnosti

V této části prosím vyplňte, jak často danou činnost provozujete, na jaké úrovni myslíte, že danou problematiku ovládáte a kde se s touto problematikou setkáváte a zdokonalujete se v ní.

X – Nikdy A – Méně jak jednou měsíčně B – Měsíčně C – Týdenně D – Denně

1 - Začátečník 2 - Středně pokročilý 3 – Pokročilý

	X,A,B,C,D	1,2,3	Místo, kde se s problematikou setkáváte
Instalace HW			
Instalace SW			
Diagnostika systému			
Nastavení operačního systému			
Znalost bezpečnostního chování			
Správa logů			
Správa zálohy			
Instalace pasivní vrstvy sítě			
Správa sítě			
Rozpoznání škodlivých programů			
Obnovení systému			

Část 3: Pracovní povinnosti

1. Jste povinni:
   a. Instalace antiviru ANO NE
   b. Správa antiviru ANO NE
   c. Údržba antiviru ANO NE
2. Jste povinni instalovat:
   a. Kabeláž systému ANO NE
   b. Stolní počítače ANO NE
   c. HW v oblasti bezpečnosti ANO NE

d. SW v oblasti bezpečnosti ANO NE

3. Máte zodpovědnost v oblasti bezpečnosti informací nebo systémové bezpečnosti?
    a. Pokud ano, upřesněte:

        _____

        _____

V následujících bodech napište, jaké si myslíte, že jsou oblasti, ve kterých byste se potřebovali zdokonalit nejvíce nebo ve kterých oblastech myslíte, že jsou vzhledem k vaší pozici důležité znát důkladněji.

1 _____

2 _____

3 _____

Příloha IV

Uvedené hodnoty jsou dané pouze jako názorný příklad

Seznam aktiv

Sériové číslo	Aktivum	Lokace	Vlastník	Odpovědná osoba	Uživatel	Číslo aktiva
S15050	Firemní notebook A	P250	škola	Karel Novák	Karel Novák	1
S123557	Server	Serverovna	škola	Jan Novák	Jan Novák	2
TL565523	Stolní počítač	P147	škola	Jana Nováková	Pavel Novák	3
S26955	Smlouvy zaměstnanců	P123	škola	Jan Novák	-	4

Tabulka odhadu rizika

Sériové číslo	Aktivum	Hrozba	P	Dopad	Úroveň rizika (H*P*D)	Existující kontroly	Osoba odpovědná za riziko	Plánované kontroly pro snížení rizika
S15050	Firemní notebook A	4	0.3	2	2.4	NE	Karel Novák	NE
S123557	Server	2.5	0.4	4	4	ANO	Jan Novák	Zabezpečení serverovny
TL565523	Stolní počítač	2.4	0.6	2.5	3.6	ANO	Jana Nováková	Pravidelný upgrade
S26955	Smlouvy zaměstnanců	2.9	0.5	3.2	4.64	NE	Jan Novák	Zavedení elektronických záloh

Příloha V

Leták do škol ke zvyšování bezpečnostního povědomí pro žáky základní školy.

SAE leták (33)